

**A COMPARATIVE STUDY OF TECHNOLOGICAL PROTECTION  
MEASURES IN COPYRIGHT LAW**

by

**MARLIZE CONROY**

submitted in accordance with the requirements  
for the degree of

**DOCTOR OF LAWS**

at the

**UNIVERSITY OF SOUTH AFRICA**

**PROMOTER: PROF CJ VISSER**

**NOVEMBER 2006**

A COMPARATIVE STUDY OF TECHNOLOGICAL PROTECTION  
MEASURES IN COPYRIGHT LAW

*by:* Marlize Conroy

(3274-781-0)

*Degree:* LLD

*Promoter:* Prof CJ Visser

*Summary*

Digitisation had a profound impact on the creation, reproduction, and dissemination of works protected by copyright. Works in digital format are vulnerable to infringement, and technological protection measures are accordingly applied as protection. Technological protection measures can, however, easily be circumvented, and additional legal protection against circumvention was needed.

Article 11 of the WIPO Copyright Treaty (the WCT) obliges Member States to provide adequate legal protection against the circumvention of technological measures applied to works protected by copyright. Contracting Parties must refine the provisions of Article 11 and provide for exceptions on the prohibition. Article 11 does not specify whether it pertains to only certain types of technological measures, nor does it prohibit the trafficking in circumvention devices.

The United States implemented the provisions of Article 11 of the WCT through the Digital Millennium Copyright Act of 1998 (the DMCA). Section 1201 of the DMCA prohibits the circumvention of technological measures. It is detailed and relates to two categories of technological measures - access control and copy control. It prohibits not only the act of circumvention, but also the trafficking in circumvention devices.

Article 6 of the EC Directive on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society of 2001 implements Article 11 of the WCT. Article 6 seeks to protect effective technological measures. It prohibits both the act of

circumvention and circumvention devices.

Although Article 11 of the WCT is silent on the issue of access control, it seems as if the international trend is to provide legal protection to access controls, thus indirectly creating a right to control access.

South Africa has not yet implemented Article 11 of the WCT. The South African Copyright Act of 1979 does not protect technological protection measures. The Electronic Communications and Transactions Act of 2002 (the ECT Act) provides protection against the circumvention of technological protection measures applied to digital data. The definition of Adata@ is such that it could include protected works. If applied to protected works, the anti-circumvention provisions of the ECT Act would be detrimental to user privileges.

As developing country, it seems to be in South Africa=s best interest to the implement the provisions of Article 11 in such a manner that it still allows users access to and legitimate use of works protected by copyright.

## FOREWORD

Daar is sekere dinge wat mens net in jou moedertaal kan sê, en dit wat ek in hierdie voorwoord wil sê, is vir my een daarvan. Daarom het ek besluit om my voorwoord in Afrikaans te skryf.

Eerstens wil ek my Hemelse Vader eer wat my nie net die vermoë nie, maar ook die geleentheid gegee het om sover met my studies te kon kom. Ek besef dat alles in my lewe net genade uit U Hand is.

Daarna vir Coenraad, my promotor: baie dankie dat jy ten spyte van jou druk program (en druk van my kant af!) hierdie stuk werk so noukeurig kon deurgaang, en ook die taal vir my geredigeer het. Ek waardeer nie net die tyd wat jy hieraan spandeer het nie, maar ook die mens wat jy is, en die belangstelling wat jy altyd in al jou kollegas en myself toon – ek het die jare wat ek saam met jou gewerk het terdeë geniet.

My dierbare ouers: ek dink daar is min mense wat so bevoorreg soos ek is om sulke wonderlike ouers soos julle te hê. Baie dankie vir al julle liefde, ondersteuning, hulp en motivering – nie net tydens die skryf van hierdie proefskrif nie, maar veral gedurende al die tye in my lewe toe ek julle nodig gehad het. Julle is vir my baie kosbaar en ek is so lief vir julle! En Mamma, baie dankie vir Mamma se hulp met die bind en inhandiging van my proefskrif – ek waardeer dit met my hele hart.

Vir die res van my familie en vriende – julle is wonderlik! Ek wil spesiaal dankie se vir my skoonouers (wat altwee self hul doktorsgrade behaal het) vir julle belangstelling - dit het vir my geweldig baie beteken. En ook in besonder baie dankie vir al julle liefde, en dat julle my met ope arms in julle familie verwelkom het – ek waardeer julle en is baie lief vir julle.

En laastens wil ek vir my man, Jaco, baie dankie sê. Ek kan nie aan hierdie tesis dink sonder om die briewe te onthou wat jy vir my geskryf het toe ek oorsee hiervoor was nie. Jaco, jy is die man van my drome, en jy lê my hart vol. Baie dankie vir elke volmaakte oomblik wat ons tot dusver kon deel. Jy en ons dierbare klein dogtertjie het

al my drome kom bewaarheid, en maak elke sekonde van my lewe die moeite werd.

Ek is lief vir jou, my man!

## Table of contents

### FOREWORD

### TABLE OF CONTENTS

|   |    |
|---|----|
| CHAPTER 1: INTRODUCTION .....   | 1  |
| CHAPTER 2: DIGITIZATION AND ITS IMPLICATIONS FOR THE LAW OF COPYRIGHT         |    |
| 2.1 Introduction .....  | 5  |
| 2.2 The Digitization of Works .....   | 5  |
| 2.2.1 The Impact of Digitization on the Format of Works .....                 | 6  |
| 2.2.2 The Impact of Digitization on Uses of Works .....                       | 7  |
| 2.2.3 The Impact of Digitization on the Distribution of Works .....           | 9  |
| 2.3 Digitization and the Rights of Authors .....                              | 12 |
| 2.3.1 The Impact of Digitization on Economic Rights .....                     | 12 |
| 2.3.1.1 The Economic Right of Reproduction .....                              | 13 |
| 2.3.1.2 The Economic Right of Distribution .....                              | 14 |
| 2.3.2 The Impact of Digitization on Moral Rights .....                        | 15 |
| 2.3.2.1 The Moral Right of Attribution .....                                  | 15 |
| 2.3.2.2 The Moral Right of Integrity .....                                    | 16 |
| 2.3.3 The Impact of Digitization on the Enforcement of Rights .....           | 17 |
| 2.3.3.1 Identifying Infringers .....  | 18 |
| 2.3.3.2 Jurisdiction .....  | 18 |
| 2.3.3.3 Choice of Law .....   | 19 |
| 2.3.3.4 The Enforcement of Judgments .....                                    | 21 |
| 2.3.4 Maintaining the Copyright Balance .....                                 | 21 |
| 2.4 New Strategies for Protecting Copyright in the Digital Age .....          | 22 |
| 2.4.1 Strategies employed by Authors to Protect Their Works .....             | 23 |
| 2.4.1.1 Contractual Conditions .....  | 24 |
| 2.4.1.2 Technological Protection .....  | 26 |
| 2.4.1.2.1 Technological Protection Measures .....                             | 28 |
| 2.4.1.2.1.1 Access Control .....  | 29 |
| 2.4.1.2.1.2 Copy Control .....  | 31 |
| 2.4.1.2.2 Rights Management Information .....                                 | 33 |
| 2.4.1.2.2.1 Authenticity and Integrity Protection .....                       | 34 |
| 2.4.1.2.2.2 Usage Metering .....  | 36 |
| 2.4.1.3 Inadequacy of Strategies Employed by Authors .....                    | 36 |
| 2.4.2 The Need for Negotiated Cross-Industry Agreements and Licences .....    | 38 |
| 2.4.3 The Need for Statutory Regulation .....                                 | 40 |
| 2.4.3.1 Anti-intellectual Property Response .....                             | 43 |
| 2.4.3.2 Intellectual Property Response .....                                  | 45 |
| 2.5 Conclusion: The WIPO Copyright Treaty .....                               | 47 |
| CHAPTER 3: THE CREATION OF NEW INTERNATIONAL NORMS: THE WIPO COPYRIGHT TREATY |    |
| 3.1 Background .....  | 48 |
| 3.2 Interpreting the WCT .....  | 52 |
| 3.3 Technological Protection Measures .....                                   | 54 |

|   |    |
|---|----|
| 3.3.1 The Proposals for the Prohibition on Circumvention Devices .....                      | 55 |
| 3.3.1.1 The United States Proposal .....  | 55 |
| 3.3.1.2 The European Commission Proposal .....  | 60 |
| 3.3.1.3 The African Proposal .....  | 61 |
| 3.3.1.4 Article 13 of the Basic Proposal for the Substantive Provisions of the Treaty ..... | 61 |
| 3.3.2 The Final Text of the WCT .....   | 68 |
| 3.3.2.1 Article 11 of the WCT .....   | 69 |
| 3.3.2.2 Limiting Article 11 .....   | 75 |
| 3.3.2.3 Enforcing Article 11 .....  | 77 |
| 3.4 Objections to the WCT .....   | 81 |
| 3.5 Conclusion .....  | 82 |

#### CHAPTER 4: THE UNITED STATES OF AMERICA

|   |     |
|---|-----|
| 4.1 Introduction .....  | 84  |
| 4.2 Preparations for Law-Making in the Information Era .....                                | 87  |
| 4.2.1 The Green Paper .....   | 88  |
| 4.2.2 The White Paper .....   | 89  |
| 4.2.3 The Proposal for the Protocol to the Berne Convention .....                           | 92  |
| 4.3 The Digital Millennium Copyright Act .....  | 93  |
| 4.3.1 Background .....  | 93  |
| 4.3.2 Technological Protection Measures .....   | 97  |
| 4.3.3 The Prohibition .....   | 100 |
| 4.3.3.1 The Prohibition on Conduct .....  | 100 |
| 4.3.3.2 The Prohibition on Trafficking in Circumvention Devices .....                       | 102 |
| 4.3.3.2.1 The Manufacture and Distribution of Devices that Circumvent Access Controls ..... | 109 |
| 4.3.3.2.2 The Manufacture and Distribution of Devices that Circumvent Copy Controls .....   | 112 |
| 4.3.4 Responsibility of Equipment Manufacturers .....                                       | 114 |
| 4.3.5 Obligations of Authors .....  | 116 |
| 4.3.6 Limiting the Application of Section 1201 .....  | 117 |
| 4.3.6.1 Ongoing Monitoring .....  | 118 |
| 4.3.6.1.1 Rule-making by the Librarian of Congress .....                                    | 118 |
| 4.3.6.1.1.1 The Initial Rule-Making Proceeding .....  | 120 |
| 4.3.6.1.1.2 The Second Rule-Making Proceeding .....   | 121 |
| 4.3.6.1.1.3 The Third Rule-Making Proceeding .....  | 124 |
| 4.3.6.1.2 Study Concerning Encryption Research and Technology .....                         | 132 |
| 4.3.6.2 The Savings Clauses .....   | 133 |
| 4.3.6.2.1 Section 1201(c)(1) and fair use .....   | 133 |
| 4.3.6.2.2 Section 1201(c)(2) .....  | 139 |
| 4.3.6.3 Exceptions to Authorize Legitimate Circumvention .....                              | 140 |
| 4.3.6.3.1 Non-profit Libraries, Archives and Educational Institutions .....                 | 140 |
| 4.3.6.3.2 Law Enforcement and Intelligence Activities .....                                 | 141 |
| 4.3.6.3.3 Reverse Engineering .....   | 141 |
| 4.3.6.3.4 Encryption Research .....   | 145 |
| 4.3.6.3.5 Protection of Minors .....  | 148 |
| 4.3.6.3.6 Personal Privacy .....  | 150 |
| 4.3.6.3.7 Security Testing .....  | 151 |
| 4.3.7 Remedies .....  | 153 |

|   |     |
|---|-----|
| 4.3.7.1 Civil Remedies .....                                  | 153 |
| 4.3.7.2 Criminal offences and penalties .....                 | 154 |
| 4.3.8 Summarizing the Objections to the DMCA Amendments ..... | 155 |
| 4.4 Conclusion .....  | 160 |

## CHAPTER 5: EUROPEAN UNION

|   |     |
|---|-----|
| 5.1 Introduction .....  | 166 |
| 5.2 Preparations for Law Making in the Information Era .....  | 168 |
| 5.2.1 The European Community Green Paper of July 1995 on Copyright and Related Rights in the Information Society .....  | 168 |
| 5.2.2 The EC Proposal for the Protocol to the Berne Convention .....  | 171 |
| 5.2.3 The EC Follow-up Paper to the Green Paper on Copyright and Related Rights in the Information Society .....  | 171 |
| 5.2.4 Proposal for a European Parliament and Council Directive on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society .....         | 174 |
| 5.2.5 Amended proposal for a European Parliament and Council Directive on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society ..... | 180 |
| 5.3 The Copyright Directive .....   | 186 |
| 5.3.1 Background .....  | 186 |
| 5.3.2 Technological Protection Measures .....   | 187 |
| 5.3.3 The Prohibition .....   | 190 |
| 5.3.3.1 The Prohibition on Conduct .....  | 190 |
| 5.3.3.2 The Prohibition on Devices .....  | 192 |
| 5.3.4 The Responsibility of Equipment Manufacturers .....   | 195 |
| 5.3.5 The Obligations of Authors .....  | 195 |
| 5.3.6 Limiting the Application of Article 6 .....   | 196 |
| 5.3.6.1 Ongoing Monitoring .....  | 196 |
| 5.3.6.2 The Savings Clauses .....   | 197 |
| 5.3.6.3 Exceptions to Legitimize Circumvention .....  | 197 |
| 5.3.6.3.1 Certain Copyright Exceptions .....  | 199 |
| 5.3.6.3.2 Private Copying .....   | 207 |
| 5.3.6.3.3 Circumvention Devices Made Available by Authors .....   | 211 |
| 5.3.6.3.4 The Interface of Copyright Law and the Law of Contract .....  | 212 |
| 5.3.6.3.5 The Relationship Between Article 6.4 and Other Directives .....   | 215 |
| 5.3.7 Remedies .....  | 218 |
| 5.3.8 A Summary of the Objections Against Article 6 .....   | 219 |
| 5.4 Conclusion .....  | 221 |

## CHAPTER 6: SOUTH AFRICA

|  |     |
|--|-----|
| 6.1 Introduction .....   | 223 |
| 6.2 Digitization and Developing Countries .....                        | 223 |
| 6.3 Copyright Protection, Human Rights, and Developing Countries ..... | 228 |
| 6.4 Current South African Legislation .....                            | 228 |
| 6.4.1 The Constitution of the Republic of South Africa .....           | 229 |
| 6.4.2 The Copyright Act .....  | 231 |
| 6.4.2.1 Direct Infringement .....                                      | 231 |
| 6.4.2.2 Contributory Liability .....                                   | 232 |
| 6.4.3 The Electronic Communications and Transactions Act .....         | 233 |

|   |     |
|---|-----|
| 6.5 A Possible South Africa-United States Free Trade Agreement? ..... | 236 |
| 6.6 Conclusion .....  | 237 |

## CHAPTER 7: THE EMERGENCE OF AN ACCESS RIGHT

|   |     |
|---|-----|
| 7.1 Introduction .....  | 239 |
| 7.2 Access in the Analogue World and Access in the Digital World .....      | 240 |
| 7.3 An Exclusive Access Right in the Analogue Environment? .....            | 243 |
| 7.4 An Exclusive Access Right in the Digital Environment? .....             | 244 |
| 7.5 The Emergence of an Access Right .....                                  | 245 |
| 7.5.1 The WIPO Copyright Treaty .....                                       | 245 |
| 7.5.2 The United States of America .....                                    | 248 |
| 7.5.3 The European Union .....  | 250 |
| 7.5.3.1 The Database Directive and the Computer Programs Directive .....    | 251 |
| 7.5.3.2 The Copyright Directive .....                                       | 251 |
| 7.5.3.2.1 Article 2 .....   | 252 |
| 7.5.3.2.2 Article 6 .....   | 252 |
| 7.5.4 South Africa .....  | 254 |
| 7.5.4.1 The Constitution of the Republic of South Africa .....              | 254 |
| 7.5.4.2 The Electronic Communications and Transactions Act .....            | 255 |
| 7.6 Distinguishing Between Unauthorized Access and Circumvention .....      | 257 |
| 7.7 Users and the Access Right .....  | 258 |
| 7.7.1 Consequences of the Access Right .....                                | 258 |
| 7.7.2 The Emergence of a Corresponding User ‘Right’ to Demand Access? ..... | 266 |
| 7.8 Conclusion .....  | 269 |

## CHAPTER 8: CONCLUSION AND RECOMMENDATIONS

|   |     |
|---|-----|
| 1 Introduction .....  | 272 |
| 2 Recommendations for Amending Legislation Generally .....                              | 272 |
| 2.1 Prohibit the Act of Circumvention, not Circumvention Devices .....                  | 273 |
| 2.2 Create a General >Other Legitimate Purposes= Exception .....                        | 274 |
| 2.3 Fair Use by Design .....  | 276 |
| 2.4 The Infringement Criterion .....  | 277 |
| 2.5 A Knowledge Requirement .....   | 279 |
| 2.6 Regulated Circumvention Devices .....   | 280 |
| 2.7 Agreements and Licences .....   | 282 |
| 2.8 Reasonableness or Proof of Damages .....  | 283 |
| 2.9 Levies .....  | 283 |
| 2.10 Alternative Business Models .....  | 285 |
| 2.11 Intermediary / Collecting Society Model .....                                      | 286 |
| 3 Recommendations for the Implementation of Article 11 of the WCT in South Africa ..... | 286 |
| 3.1 Should South Africa Implement Article 11? .....                                     | 287 |
| 3.2 Exclude the Operation of the Electronic Communications and Transactions Act .....   | 287 |
| 3.3 Amend the Copyright Act .....   | 288 |
| 3.3.1 Definitions .....   | 288 |
| 3.3.2 The Circumvention Prohibition .....   | 288 |
| 3.3.3 Exceptions .....  | 290 |
| 4 A Final Teaser .....  | 291 |

BIBLIOGRAPHY

INDEX

## CHAPTER 1: INTRODUCTION

‘Dear, dear! How queer everything is today!  
And yesterday things went on just as usual,  
I wonder if I’ve changed in the night?’

LEWIS CARROL

*Alice’s Adventures in Wonderland*

It sometimes feels as if we, like Alice, have slipped down a rabbit-hole and woke up in Wonderland. Our Wonderland is called Cyberspace, a place with no borders and seemingly very few rules. But it is a wonderful place, a place of opportunity! But although Cyberspace is a land of many opportunities, it is important to regulate Cyberspace to safeguard its inhabitants.

Living in Cyberspace affects all aspects of our lives. It affects how we entertain ourselves, how we communicate, how we transact, and how we create. So one comprehensive set of rules would be insufficient to regulate all these aspects. Specific legislation aimed at each aspect is needed.

The focus of my thesis will be on the regulation of one such aspect only – how we create in Cyberspace. Traditionally, the protection of the rights of a creator is regulated by copyright law. I will examine a facet of the copyright protection of creative works – technological protection measures, and the corresponding unlawful circumvention of these measures. I shall concern myself only with copyright law and so the circumvention of protection measures applied to information protected by the law of privacy falls outside the scope of my thesis.

In Chapter 2, I shall start my discussion with an overview of the new technologies that lead to the creation of Cyberspace. I shall discuss the phenomenon of digitization and its impact on the creation, reproduction, and dissemination of works protected by copyright. Because of the specific nature of works in digital format, they are especially vulnerable to misuse. So technological protection measures are applied to digital works to safeguard them against

infringement. Since these measures can easily be circumvented, additional legal protection against their circumvention is needed. After much debate, it was decided that technological protection measures, like the works that they enclose, should be regulated by copyright law. And since Cyberspace transcends geographic frontiers, an international regime had to be established to protect technological protection measures against circumvention. In Chapter 3 I shall discuss the international context. I shall refer, especially, to the WIPO Copyright Treaty. Article 11 of this treaty obliges Contracting Parties to provide adequate legal protection against the circumvention of technological protection measures that are applied to works protected by copyright. This provision is formulated in a broad and technologically neutral way, and leaves it to Contracting Parties, on implementation, to refine its provisions and to provide for exceptions to the prohibition..

Before I turn to the position in South Africa, I shall look at the implementation of the WIPO Copyright Treaty in two jurisdictions – the United States of America, and the European Union.

In Chapter 4, I shall canvass the implementation of the WIPO Copyright Treaty in the United States. It was one of the first developed countries to ratify the WCT. The United States belongs to the common law copyright family, in which copyright is seen as a kind of ownership. So literary and artistic works are protected by copyright law to provide authors with an incentive to create more works. As South Africa likewise belongs to the common-law family, and since the United States was one of the first countries to implement the WCT, I think it prudent to investigate the American implementing legislation, notably, the amendment of the Copyright Act by the Digital Millennium Copyright Act of 1998. As I shall show, the Act contains a detailed provision relating to the circumvention of technological protection measure. It not only concerns two types of technological protection measure (access control, and copy control), but strikes at both the act of circumvention and the trafficking in devices used for circumvention purposes. The Act also creates a number of exceptions to the prohibition.

Even though, as I have said, South African copyright law belongs to the common-law family, it also has certain characteristics borrowed from the civil-law family, in which copyright is

seen as an extension of the author's personality, and protected as such. To contrast the common and civil-law copyright families, in Chapter 5, I shall canvass the implementation of the WIPO Copyright Treaty in the European Union. (Most of its Member States belong to the civil-law family.) Also, the legislative instruments of the European Union have had a profound impact on international copyright law. So I shall pay close attention to article 6 of the EC Directive on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society of 2001. I shall show that the exceptions stated in article 6 are not mandatory (bar one), which may yet defeat the purpose of harmonizing copyright law in the European Union.

In Chapter 6, I shall turn to South Africa. I shall show that, currently, South Africa has no legislation specifically aimed at regulating the copyright protection of digital works. The Copyright Act of 1978 was drafted with analogue works in mind, but its infringement provisions apply with equal force to digital works. It is silent as to technological protection measures of copyright works. Other legislation that may impact on the issue under discussion, are the Constitution of the Republic of South Africa, 1996, and the Electronic Communications and Transactions Act of 25 of 2002. The Constitution protects, amongst others, the right to property, the right to education, and the right of access to information. The Electronic Communications and Transactions Act deals with the integrity of digital information, which may, of course, include digital copyright works.

In Chapter 7, I will examine the emergence of an access right. The access right is a new right in the context of copyright law and emerged as a consequence of the prohibition on the circumvention of access controls.

The special focus of my thesis, then, is on how article 11 of the WIPO Copyright Treaty should be implemented in South Africa. On the basis of the legislative experiences in the United States of America and the European Union, I shall determine whether an express new prohibition on circumvention in copyright law is actually necessary, and, if it is, what legislative language would be appropriate. In this process I shall consider not only the wording of the prohibition but also any exceptions and limitations that may be appropriate to maintain the often elusive copyright balance. In Chapter 8 I shall advance my legislative

proposals.

## CHAPTER 2: DIGITIZATION AND ITS IMPLICATIONS FOR COPYRIGHT LAW

“Curiouser and curiouser!” cried Alice (she was so much surprised, that for the moment she quite forgot how to speak good English)...’

LEWIS CARROL

*Alice’s Adventures in Wonderland*

### 2.1 Introduction

The increased importance of computer programs, computer-generated works, and databases, and the development of digital transmissions systems (such as the Internet) changed the world around us.<sup>1</sup> Indeed, these developments turned the world of the early 1970s into the Wonderland we know today.<sup>2</sup> And this Wonderland of ours, cyberspace is indeed a curious place to be.

In this chapter I shall start with a brief description of the technological developments during the past 30 years and how these developments offer new opportunities to create and enjoy works. I shall focus on the digitization of works, which process impacted not only on the creation and use of works but also on their distribution. I shall then indicate how these new developments have resulted in misuse to infringe on the authors’ rights.<sup>3</sup> Finally, I shall discuss the different solutions to the problem of protecting copyright works in cyberspace.

### 2.2 The Digitization of Works

It sometimes seems as if we have forgotten how to speak English in this curious new world of

---

<sup>1</sup> Wend Wendland ‘The Digital Agenda’ (1997) 5 *JBL* 143 at 143.

<sup>2</sup> Development has not stopped here. New technologies and techniques keep surfacing. Advances in compression technology mean, for example, that it will become increasingly easier, faster and more convenient to digitally transmit full-length high-quality audio and video works. Increases in bandwidth mean greater capacity for delivering more data more quickly. It will make it easier to distribute high quality works with little time or cost factor. Dean S Marks & Bruce H Turnbull ‘Technical Protection Measures: The Intersection of Technology, Law and Commercial Licences’ [2000] *European Intellectual Property Review* 198 at 199.

<sup>3</sup> For purposes of this writing I will use the term ‘author’ to refer to both authors as well as copyright owners, even though these terms are not synonymous. The term ‘author’ usually refers to the first maker or creator of a work, whereas ‘copyright owner’ refers to the person or entity entitled to exercise the economic rights over the copyright work.

ours. So it is important briefly to explain of the meaning of one of the new terms that we have created for our new world. 'Digitization' is perhaps the most significant of recent technological developments. It connotes the conversion of works to a format in which they can be read by a machine.<sup>4</sup> Digitization, then, is basically the ability to record works in a binary format (a sequence of ones and zeros) in which they are stored and transmitted. There are different methods of digitizing works but they all have the same result - they create a binary code that can be 'played back' to reproduce the original analogue experience.<sup>5</sup> All tangible works, no matter how complicated, can be recorded in digital format. Digitization thus creates a 'common form' in which all types of subject-matter can be made available to users.<sup>6</sup>

Digitization had an impact not only on the format of works but also on their use of works and distribution.

### **2.2.1 The Impact of Digitization on the Format of Works**

In the analogue world, works were created and distributed in material forms such as books or paintings. These works were susceptible to the human senses. The copyright works as embedded in material form were protected by law of copyright. It was the expression of the idea in the material form that was protected and not the ideas underlying the expression. Accordingly reduction to material form became a requirement for copyright protection in the analogue world.

---

<sup>4</sup> A computer is not the only machine that can read digital formats. TV-sets, telephones and computers are losing their distinctive characters, and can all be used to provide digital services. Thomas K Dreier 'Convergence Through Digital Technology - The Effect on Copyright and Information Services' *10th Annual Conference on Intellectual Property Law and Policy*, 5 April 2002, 1.

<sup>5</sup> Stephen M Kramarsky 'Copyright Enforcement In the Internet Age: The Law and Technology of Digital Rights Management' (2001) 11 *De Paul - LCA Journal of Art and Entertainment Law* 1 at 3-4.

<sup>6</sup> Andrew Christie 'Reconceptualising Copyright in the Digital Era' [1995] *European Intellectual Property Review* 522 at 523; Mark Bide, Charles Oppenheim & Anne Ramsden 'Copyright Clearance and Digitization in UK Higher Education: Supporting Study for the JISC/PA Clearance Mechanisms Working Party' accessible at <<http://www.ukoln.ac.uk/services/elib/papers/pa/clearance/>> (visited on 21 November 2006) at 3-4; G Gervaise Davis III 'The Digital Dilemma: Coping with Copyright in a Digital World' (1993) 27 *Copyright World* 18; Dreier op cit note 4 at 1; and Eric Fleischmann 'The Impact of Digital Technology on Copyright Law' (1988) 70 *Journal of Patent and Trademark Office* 5 at 6. Christie refers to digitization as 'technological Latin' since it makes all works available in one common form.

Digital works, by contrast, have been ‘dematerialised’ into electronic or digital format. They are not contained in traditional material formats. Although the digital format of works can be ‘read’ or understood only by technologies such as computers, it can be readily translated into impulses susceptible by the human eye, ear, and mind.<sup>7</sup>

Any existing analogue work can be converted into a digital data object.<sup>8</sup> It is also very popular to create new works in digital format, as doing so is convenient and inexpensive.<sup>9</sup>

So works now exist either both in analogue and digital format, or only in digital format. Some of the ‘digital-born’ works, such as newsletters and original databases, are published only in digital format over networks such as the Internet and are never converted to the traditional material form of the analogue world.<sup>10</sup>

### **2.2.2 The Impact of Digitization on Uses of Works**

The conversion from analogue to digital not only revolutionized the ways in which works can be created but also the ways in which works can be used. The most significant result of digital technology is perhaps the simplicity and ease of reproduction.<sup>11</sup> Analogue copies degrade in quality with each generation of copying, and so analogue copying contains an inherent physical limitation on multi-generation copying. This serves as an obstacle to large-scale unauthorized copying. Digital copies, however, are perfect, as digital copying involves bit-for-bit replication. This means not only that every digital copy itself is perfect, but also

---

<sup>7</sup> Roger Clarke ‘Technological Protections for Digital Copyright Object’ accessible at <<http://www.anu.edu.au/people/Roger.Clarke/II/TPDCO.html>> (visited on 22 November 2006).

<sup>8</sup> This is commonly referred to as ‘digitization’. Works can be digitized by using, for example, scanners, OCR, digital cameras, and digital audio-recording (‘Digital Technology and the Copyright Act 1994: A Discussion Paper - Part Two: Background’ accessible at <[http://www.med.govt.nz/buslt/int\\_prop/digital/digital-04.html](http://www.med.govt.nz/buslt/int_prop/digital/digital-04.html)> (visited on 3 October 2002)).

<sup>9</sup> By using, for example, desktop publishing packages, PC-based graphic design tools, animation, and digital music generators.

<sup>10</sup> This is commonly referred to as ‘digitization’. Works can be digitized by using, for example, scanners, OCR, digital cameras, and digital audio-recording. Roger Clarke op cit note 7; ‘Digital Technology and the Copyright Act 1994: A Discussion Paper - Part Two: Background’ op cit note 8; Allen N Dixon & Martin F Hansen ‘The Berne Convention Enters the Digital Age’ [1996] *European Intellectual Property Review* 604 at 605; and David N Weiskopf ‘The Risks of Copyright Infringement on the Internet: A Practitioner’s Guide’ (1998) 33 *University of San Francisco Law Review* 1 at 3.

<sup>11</sup> Peter Kumik ‘Digital Rights Management’ (2001) 1 *Legal Information Management* 21.

that perfect copies can be made from other copies through endless generations.<sup>12</sup>

Analogue copying usually involves a time-consuming process on expensive equipment. Digital copying, by contrast, can be done with hardly any cost and at high speed<sup>13</sup> by everyone with a computer.<sup>14</sup>

Although the ease and perfection of digital copying poses a definite threat to authors' reproduction right, it also offers some advantages to authors. Authors can use digital copying to make higher quality copies of works such as sound recordings and films at lower unit cost.<sup>15</sup>

A further feature of digital works is the ease with which they can be manipulated and modified.<sup>16</sup> The manipulation or modification of a digital work does not degrade the quality of that work.<sup>17</sup> Works in digital form can be manipulated and modified in almost unlimited ways.<sup>18</sup> Sound recordings originally recorded in analogue format and old film prints are increasingly being digitally re-mastered and re-released.<sup>19</sup> This is made possible by digital editing techniques by means of which sounds can be altered, colour added to black-and-white films, and even the actors in a film changed.<sup>20</sup>

The ease with which digital works can be modified and combined lead to a new type of work - multimedia works. A multimedia work is basically a work that combines different types of work, or different sensory experiences, and delivers them as one work on a single medium, such as CD-Rom. Digital encyclopaedias and educational and entertainment offerings are typical examples of multimedia works.<sup>21</sup>

---

<sup>12</sup> Fleischmann op cit note 6 at 6-7 and 9-10; Marks & Turnbull op cit note 2 at 198-199.

<sup>13</sup> Marks & Turnbull op cit note 2 at 198-199.

<sup>14</sup> By using, inter alia, disk-to-disk copying, screen scrapers, and CD-burners as a consumer appliance. (Clarke op cit note 7; Marks & Turnbull op cit note 2 at 199).

<sup>15</sup> 'Digital Technology and the Copyright Act 1994: A Discussion Paper - Part Two: Background' op cit note 8.

<sup>16</sup> Using, for example, word-processors, and sound and image editing tools (Clarke op cit note 7).

<sup>17</sup> Christie op cit note 6 at 523.

<sup>18</sup> Using, for example, word-processors, and sound and image editing tools (Clarke op cit note 7).

<sup>19</sup> 'Digital Technology and the Copyright Act 1994: A Discussion Paper - Part Two: Background' op cit note 8.

<sup>20</sup> Dixon & Hansen op cit note 10 at 606.

<sup>21</sup> Ibid. These new forms of multimedia products have presented two challenges namely the categorization of works and licensing. There is no such thing as a 'multimedia work' in copyright law. Where a work exists as a combination of other works, which rules will apply? The other challenge is how to get the necessary licence to

Two additional characteristics of digital works are the ease of their storage because of digital compression, and the ease of searching and linking digital data and works.<sup>22</sup>

Because of the ease with which analogue works can be digitized, these new uses not only impact on the uses of digital works but also offer potentially new uses of works still in analogue format.<sup>23</sup>

### **2.2.3 The Impact of Digitization on the Distribution of Works**

Digital technology has altered the ways in which works are distributed. While analogue works were published in physical form and then distributed by means of air, land, or sea transport, or microwave transmissions, digital works can be delivered by means of digital transmission.<sup>24</sup> Digital transmission began with specialized news and data services, followed by commercial online services. Presently the most widespread transmission mechanism is the Internet.<sup>25</sup>

Digital transmission offers the potential that every type of work could be made available, in digital form, on an electronic network or series of networks that are accessible world wide.<sup>26</sup>

Copyright traditionally has been concerned with communication or distribution to the public in general. The transmission of works was limited to that which occurred on a one-to-one

---

include another's copyright work in a multimedia work. If someone else's copyright work is to be included in a multimedia product, a licence is needed from the relevant author. If parts of several works are to be included, several different licences are required. As a result, there have been some complaints about the 'difficulty' of multimedia licensing, and various schemes proposed to automate or centralize some licensing functions.

<sup>22</sup> Gervaise Davis III op cit note 6 at 20; Vanessa van Coppenhagen 'Copyright and the WIPO Copyright Treaty, with Specific Reference to the Rights Available in a Digital Environment and the Protection of Technological Measures' (2002) 119 *South African Law Journal* 429 at 430.

<sup>23</sup> Marks & Turnbull op cit note 2 at 198-199.

<sup>24</sup> Dixon & Hansen op cit note 10 at 606.

<sup>25</sup> Idem at 607.

<sup>26</sup> Committee on Intellectual Property Rights and the Emerging Information Infrastructure; Computer Science and Telecommunications Board; Commission on Physical Sciences, Mathematics, and Applications; National Research Council 'The Digital Dilemma: Intellectual Property in the Information Age' (2001) 62 *Ohio State Law Journal* 951; Allen N Dixon & Laurie C Self 'Copyright Protection for the Information Superhighway' [1994] *European Intellectual Property Review* 465; Dixon & Hansen op cit note 10 at 607.

basis (like telephone communication) or on a one-to-many basis (like broadcasting).<sup>27</sup> Digital transmission involves the transfer of works to individuals.<sup>28</sup> Transmission of a copyright work in digital form can now take place on a one-to-one, many-to-many, or all-to-all basis.<sup>29</sup> Works can be sent from one individual to another, from an individual to a select group, or from an individual to the public at large.<sup>30</sup> Networking and personal home devices<sup>31</sup> allow users to receive and to send works from home, and to move works among the different devices in their homes.<sup>32</sup>

Digital transmission is interactive, and so is no longer limited to that which occurs on a one-way basis.<sup>33</sup> There is no broadcaster that sends out works to be received by the public at a time of the broadcaster's choice. Instead, works are made available on a 'server' to be accessed or used at a time determined by the user. Other than making the works available, the service provider may be a passive participant. The user is the active participant by accessing, using, or copying a particular work.<sup>34</sup> The user can also, in turn, act as a further publisher of the work and so become an unauthorized re-publisher.<sup>35</sup> Digital transmission thus made true communication possible.<sup>36</sup>

While there were delays between the creation, publication, and availability of works in the analogue world, digital transmission is almost immediate.<sup>37</sup> The delays between the creation of works and their availability to users are greatly reduced. Compression (the reduction of a digital file's size) speeds up the download time of a file, which makes wide distribution even more of a reality.<sup>38</sup>

Digital transmission systems are also less expensive than comparable analogue systems. This can be ascribed to two reasons - digital works can be stored in less space than is possible with

---

<sup>27</sup> Christie op cit note 6 at 523.

<sup>28</sup> Dixon & Hansen op cit note 10 at 607.

<sup>29</sup> Christie op cit note 6 at 523.

<sup>30</sup> Dixon & Hansen op cit note 10 at 607.

<sup>31</sup> Such as personal computers, televisions, recorders and music systems.

<sup>32</sup> Marks & Turnbull op cit note 2 at 199.

<sup>33</sup> Christie op cit note 6 at 523.

<sup>34</sup> Dixon & Hansen op cit note 10 at 607.

<sup>35</sup> Marks & Turnbull op cit note 2 at 199.

<sup>36</sup> Christie op cit note 6 at 523.

<sup>37</sup> Fleischmann op cit note 6 at 8.

analogue works, and fibre optic cables carry digital transmissions more cheaply than microwave transmissions carry analogue transmissions.<sup>39</sup>

In the analogue world, copying copyright works was allowed in only defined circumstances. But digital transmissions are marked by temporary copying and uses. Interactive services often involve uses of works in which (a) no copy is delivered at all; (b) only a temporary copy is made in computer memory; (c) the only copy made exists on the hard drive of a computer; or (d) only part of a work is used, for a limited time. A user that accesses a copyright database online, for example, typically looks for only one particular type of material, which may be copied onto the user's computer for later use, or may simply be used until the user exits the database. Similarly, computer programs can be used online simply by loading them into a computer's RAM memory.<sup>40</sup>

The number of digital transmissions of copyright works handled by telecommunications carriers (like telephone companies) and similar carriers for such interactive services has increased dramatically in recent years. New intermediaries (such as online service providers) that provide a link between users and the telecommunications carrier have appeared in the delivery process.<sup>41</sup>

Not only users but also authors profit from digital transmission services. Digital transmission provides new ways to authors to distribute and market their works. Because of the speed of digital transmission, it can be used very rapidly to transmit works to the public or an individual user.<sup>42</sup> It also provides, for example, artists in the visual and performing arts with the opportunity to hold online exhibitions.<sup>43</sup> And musicians who have not been signed by record companies can bypass traditional marketing channels by posting copies of their recordings on the Internet for sale or free distribution.<sup>44</sup>

---

<sup>38</sup> Kramarsky op cit note 5 at 5-7.

<sup>39</sup> Fleischmann op cit note 6 at 8.

<sup>40</sup> Dixon & Hansen op cit note 10 at 607.

<sup>41</sup> Ibid.

<sup>42</sup> Using inter alia modem-to-modem transmission, CD-ROMs in the mail, mailed attachments, FTP-download, and web-download (Clarke op cit note 7).

<sup>43</sup> 'Digital Technology and the Copyright Act 1994: A Discussion Paper - Part Two: Background' op cit note 8.

<sup>44</sup> Ibid; Brian Leubitz 'Digital Millennium? Technological Protections for Copyright on the Internet' (2003) 11 *Texas Intellectual Property Law Journal* 417 at 418-419.

Digital transmission also creates new ways for users to use and enjoy works. Users now have inexpensive and widespread access to large numbers of works, from a variety of devices,<sup>45</sup> at locations of their choice.<sup>46</sup> An example of one of the advantages is that software and music titles are increasingly available on the Internet at the same time as physical copies are released through traditional retail outlets.<sup>47</sup>

### **2.3 Digitization and the Rights of Authors**

The benefits of digitization are endless. For authors, digitization offers not only new ways of creating works but also the wide and efficient dissemination of their works by digital transmission. For the computer, broadcasting, cable, satellite, and telecommunications industries, there is the potential for technical innovation and growth. And for virtually every member of the public, digital transmission makes works, information, and services available online in forms much more useful than the old analogue formats.<sup>48</sup>

However, despite these many advantages of digitization, time proved it to be a double-edged sword - it not only lead to new and exciting ways of creating and enjoying copyright works, but also provided new ways of infringing authors' rights.<sup>49</sup>

Digitization threatens authors' economic and moral rights, as well as their enforcement. It also poses the threat of upsetting the existing balance between the rights of authors and those of users.

#### **2.3.1 The Impact of Digitization on Economic rights**

Copyright grants authors certain exclusive rights of authorization. Where someone performs

---

<sup>45</sup> Such as PCs, PDAs, mobile phones, public kiosks, and web-enabled TV (Clarke op cit note 7).

<sup>46</sup> Such as the workplace, the home, public kiosks and Internet cafés. Ibid; 'Digital Technology and the Copyright Act 1994: A Discussion Paper - Part Two: Background' op cit note 8.

<sup>47</sup> Ibid.

<sup>48</sup> Dixon & Self op cit note 26 at 465.

<sup>49</sup> Marks & Turnbull op cit note 2 at 198; 'Digital Technology and the Copyright Act 1994: A Discussion Paper - Part Two: Background' op cit note 8.

any of the restricted acts without the author's authority, such person infringes on the author's copyright. The granting of these exclusive rights allows authors to control their works and to exploit it economically.<sup>50</sup>

Many, if not all, of an author's economic rights are likely to be affected by digital technology in some way or the other. For purposes of this discussion I will, however, only focus on some of the effects of digitization on the economic rights of reproduction and distribution.

### **2.3.1.1 The Economic Right of Reproduction**

The effect of digitization on the author's reproduction right is obvious. Digitization itself always includes reproducing a work. The mere conversion of a copyright work to digital format can constitute copyright infringement if it is done without the author's consent.<sup>51</sup>

As I have indicated, in the analogue world the threat of reproduction was limited because analogue technology by its nature prevented making inexpensive and high-quality copies.<sup>52</sup> Digital and optical disk technology, by contrast, enables the making of unlimited numbers of high-quality copies at a comparatively low cost. The quality of digital copies makes it difficult to detect copying, as it is not easy to identify whether a work is original or merely a copy of the original work.<sup>53</sup> This facilitates widespread copying.

In the analogue world, copying was time consuming whereas digital copying is instantaneous.

---

<sup>50</sup> 'Digital technology and the Copyright Act 1994: A Discussion Paper - Part Two: Background' op cit note 8.

<sup>51</sup> Michael Lehmann 'Digitisation and Copyright Agreements' in Dr Irini A Stamatoudi & Paul LC Torremans (eds) *Perspectives on Intellectual Property: Copyright in the New Digital Environment* 2000 London: Sweet & Maxwell 195 at 195.

<sup>52</sup> Committee on Intellectual Property Rights and the Emerging Information Infrastructure; Computer Science and Telecommunications Board; Commission on Physical Sciences, Mathematics, and Applications; National Research Council op cit note 26 at 953; TC Vinje 'A Brave New World of Technical Protection Systems: Will There Still be Room for Copyright?' [1996] *European Intellectual Property Review* 431.

<sup>53</sup> See, for example, Cynthia M Botte 'Protection of Information Products: Balancing Commercial Reality and the Public Domain' (1998) 67 *University of Cincinnati Law Review* 237 at 245; 'Digital technology and the Copyright Act 1994: A Discussion Paper - Part Two: Background' op cit note 8; and David Nimmer 'A Tale of Two Treaties Dateline: Geneva - December 1996' (1997) 22 *Columbia - VLA Journal of Law and the Arts* 1 at 5.

The nature of analogue copy technologies lead to the assumption that copying technologies (such as photocopiers and audio or video cassette recorders) only had limited economic effect on the author. Reproduction for ‘private study’ and similar exceptions was thus permitted.<sup>54</sup> In the digital world, however, anyone with the widely available technology can make an unlimited number of unauthorized copies of a work.<sup>55</sup> Digital copy technologies have a profound impact on the rights of an author, and the question arose whether exceptions to the right of reproduction should still be permitted.

Unauthorized digital reproduction does not require the physical distribution channels of the past such as flea markets, corner shops, or retail outlets to distribute unauthorized copies. In the digital world, nearly anyone with the necessary equipment can distribute unauthorized copies of a work through digital transmission.<sup>56</sup>

It has been argued that the public has always believed that unauthorized copying is socially acceptable behaviour. The digitization of works is not likely to change this attitude. Rather, the ease and perfection of digital copying will make reproduction far easier than it was in the analogue world.<sup>57</sup>

The availability of unauthorized perfect copies impacts on the market for copyright works<sup>58</sup> and threatens authors’ revenue streams. This can detrimentally affect decisions to create, invest in, and distribute copyright works.<sup>59</sup>

### **2.3.1.2 The Economic Right of Distribution**

Copies of a work can easily be distributed or made available to the public through digital transmission systems such as the Internet. By publishing online, a work is not only made

---

<sup>54</sup> Dixon & Hansen op cit note 10 at 605; Kumik op cit note 11 at 21.

<sup>55</sup> Angela Bowne ‘Trade Marks and Copyright on the Internet’ (1997) 2 *Media and Arts Law Review* 135 at 135; Marks & Turnbull op cit note 2 at 199.

<sup>56</sup> Ibid.

<sup>57</sup> Fleischmann op cit note 6 at 11-12.

<sup>58</sup> Idem at 5.

<sup>59</sup> ‘Digital technology and the Copyright Act 1994: A Discussion Paper - Part Two: Background’ op cit note 8.

available to potential customers but also exposed to potential pirates.<sup>60</sup> A further threat is that an author exposes herself to the possibility that someone can interfere with the publication of her work, for example, by preventing it from reaching its intended destination.

The greatest threat is perhaps that by publishing on the Internet, an author can lose control of the distribution of her work.<sup>61</sup> It is almost impossible to control the exploitation of copyright works in cross-border, global information networks such as the Internet. The reason for this is that each recipient can also become a provider with worldwide reach; it is possible for anyone not only to access databases but to act as a database herself.<sup>62</sup>

The effect of a lost control of distribution is that an author will get paid only for a small percentage of the uses of her work.<sup>63</sup>

### **2.3.2 The Impact of Digitization on Moral Rights**

An author has, independently of her economic rights, and even after transfer of her economic rights, moral rights in her works.<sup>64</sup> The two principal moral rights are the right of attribution, and the right of integrity.<sup>65</sup> Digital technology also eased the ways in which these rights can be infringed.<sup>66</sup>

#### **2.3.2.1 The Moral Right of Attribution**

---

<sup>60</sup> Ibid.

<sup>61</sup> Kumik op cit note 11 at 21.

<sup>62</sup> Committee on Intellectual Property Rights and the Emerging Information Infrastructure; Computer Science and Telecommunications Board; Commission on Physical Sciences, Mathematics, and Applications; National Research Council op cit note 26 at 954; Thomas Dreier 'Copyright Law and Digital Exploitation of Works' accessible at <<http://www.fes.de/fulltext/stabsabteilung/00218001.htm>> (visited on 3 October 2002).

<sup>63</sup> Kumik op cit note 11 at 21.

<sup>64</sup> Originally, moral rights were recognized only in the Continental legal systems. Article 6bis of the Berne Convention regulates moral rights. The TRIPS Agreement obliges contracting parties to comply with articles 1 to 21 of and the Appendix to the Berne Convention but exempts article 6bis of the Berne Convention. However, as will be seen later, the WIPO Copyright Treaty obliges contracting parties to comply with all the above articles as well as article 6bis (see further Jörg Reinbothe & Silke von Lewinski 'The WIPO Treaties 1996: Ready to Come into Force' [2002] *European Intellectual Property Review* 199 at 200.

<sup>65</sup> Article 6bis(1) of the Berne Convention.

<sup>66</sup> See 'Digital technology and the Copyright Act 1994: A Discussion Paper - Part Two: Background' op cit note 8; and JAL Sterling 'Philosophical and Legal Challenges in the Context of Copyright and Digital

The right of attribution is the right to be identified as the author of a work.<sup>67</sup>

Because of the ease by which digital works can be manipulated, the right of attribution in works created in or converted to digital format is at risk - during the conversion from analogue to digital format an author's name can be removed or altered.<sup>68</sup>

A work in digital format, whether it was created in or converted to digital form, can easily be manipulated. A work distributed over the Internet is especially at risk. An author's name can be altered or removed from her work at any stage of transmission over the Internet.<sup>69</sup> Not only can an author's name be altered or removed during transmission but an anonymous author's identity can also be revealed. Techniques of tracking the source of material placed on web sites may render it more difficult for the author to maintain anonymity, where it is desired.<sup>70</sup>

The ease of removal or alteration of an author's name makes determining the authenticity of material placed on the Internet difficult, if not impossible, as far as users are concerned. How can a user determine whether what is said to be the work of the author is actually such?<sup>71</sup>

### **2.3.2.2 The Moral Right of Integrity**

The right of integrity is the right to object to any distortion, mutilation, or other modification of a work where that treatment is prejudicial to the honour or reputation of an author.<sup>72</sup>

The creation of a work in digital format, or the conversion of an analogue work into digital format, can also infringe the author's right of integrity.<sup>73</sup> A digital work can be manipulated in endless ways. Any such manipulation can, however, amount to an infringement of the

---

Technology' (2000) 31 *International Review of Industrial Property and Copyright Law* 508 at 518.

<sup>67</sup> In terms of article 6bis(1) of the Berne Convention, an author has 'the right to claim authorship of the work'.

<sup>68</sup> 'Digital technology and the Copyright Act 1994: A Discussion Paper - Part Two: Background' op cit note 8.

<sup>69</sup> Sterling op cit note 66 at 519.

<sup>70</sup> Ibid.

<sup>71</sup> Ibid.

<sup>72</sup> In terms of article 6bis(1) of the Berne Convention, an author has 'the right to ... object to any distortion, mutilation or other modification of, or other derogatory action in relation to, the said work, which would be prejudicial to his honor or reputation'.

author's right to preserve the integrity of the work.<sup>74</sup>

Once a work has been distributed on the Internet, anyone who can access the Internet is in a position to resize, re-colour, or manipulate copies of the work in many other ways. Authors are likely to have difficulties exercising their moral rights to object to derogatory treatment of their works that they consider harmful to their honour or reputation where copies are widely distributed over the Internet.<sup>75</sup>

Again the user is also adversely affected: How will the user be able to identify unauthorized insertions into or deletions from her work?<sup>76</sup>

### **2.3.3 The Impact of Digitization on the Enforcement of Rights**

Copyright has territorial application and the international conventions are built upon this premise.<sup>77</sup> Despite the existence of international conventions there is considerable variation in national laws, enforcement policies, and cultural attitudes towards intellectual property. And fundamental legal concepts can be interpreted differently in different countries.<sup>78</sup> Information networks, however, have global reach and the borders between countries are disappearing. So the traditional copyright enforcement procedures are not adequate to deal with infringement in cyberspace.

Authors are thus faced with the problem of detecting infringement as well as the question of how to enforce their rights once they have been infringed.

Four main problems surface in this context: identifying infringers, determining jurisdiction,

---

<sup>73</sup> 'Digital technology and the Copyright Act 1994: A Discussion Paper - Part Two: Background' op cit note 8.

<sup>74</sup> Sterling op cit note 66 at 519.

<sup>75</sup> 'Digital technology and the Copyright Act 1994: A Discussion Paper - Part Two: Background' op cit note 8.

<sup>76</sup> Sterling op cit note 66 at 519.

<sup>77</sup> Idem at 521-522; and Raquel Xalabarder 'Copyright: Choice of Law and Jurisdiction in the Digital Age' (2002) 8 *Annual Survey of International and Comparative Law* 79-96 at 80.

<sup>78</sup> Committee on Intellectual Property Rights and the Emerging Information Infrastructure; Computer Science and Telecommunications Board; Commission on Physical Sciences, Mathematics, and Applications; National Research Council op cit note 26 at 955.

determining the applicable law, and enforcing judgments against infringers.<sup>79</sup>

### **2.3.3.1 Identifying Infringers**

The first question is who should be held liable for copyright infringement in the digital environment.

More often than not, home equipment is used to commit digital copyright infringement. This makes it difficult not only to detect infringement but also to prove infringement, especially in the light of privacy considerations.<sup>80</sup>

Weiskopf<sup>81</sup> illustrates a further problem in this regard by means of the following example:

‘When someone uploads a copyrighted picture without authority onto a Web site, many people, not just one, will likely visit the site. . . . [E]ach visit or “hit” to the Web site potentially constitutes a new infringement of one or more exclusive rights of the copyright owner. Thus, there are potentially hundreds, thousands or even millions of infringers as a result of one infringing work posted to the Internet. However, imposing liability on any or all of these visitors may be practically impossible. Indeed, because people can operate with almost complete anonymity in cyberspace, identifying infringers can be difficult. Additionally, physically locating the accused violator can be impossible, even if one could determine their “cyberspace address”.’

Because of the difficulties involved in holding each separate individual infringer liable, three classes of Internet users are emerging upon which liability is being regularly imposed for infringement on the Internet: online service providers (including access and content providers), the operators of bulletin boards, and web-site operators.<sup>82</sup>

### **2.3.3.2 Jurisdiction**

---

<sup>79</sup> Sterling op cit note 66 at 522.

<sup>80</sup> See, generally, Lee A. Bygrave ‘The Technologicalisation of Copyright: Implications for Privacy and Related Interests’ [2002] *European Intellectual Property Review* 51-57; Fleischmann op cit note 6 at 9-11.

<sup>81</sup> Weiskopf op cit note 10 at 6-7.

The Berne Convention does not provide for any rule of jurisdiction concerning copyright infringement.<sup>83</sup> Copyright law and the rules of private international law are used to determine jurisdiction and choice of law in cases where a foreign element is involved. It is based on the premise that copyright is territorial.<sup>84</sup>

The digital world, by contrast, has no respect for traditional geographic borders. The determination of the place and manner of unauthorized reproduction and adaptation, and of dissemination and communication to the public, involves problems that, in the present state of international law, are intractable.<sup>85</sup> This may make bringing an infringement action very difficult in many circumstances.<sup>86</sup>

The fact that infringement on the same work can take place simultaneously in several foreign countries compounds the problem. In which jurisdiction should the author institute action?<sup>87</sup> Or should action be instituted in several jurisdictions simultaneously? The cost of litigation in many legal systems, often with widely differing standards, may deter authors from participating in an electronic marketplace, as they will not be able to enforce their rights.<sup>88</sup>

The problems relating to jurisdiction can also create a situation in which authors will choose their forum based on vagaries of procedure here and there. Courts should not be bothered with these types of consideration, as it creates needless side-tracking.<sup>89</sup>

### **2.3.3.3 Choice of Law**

Article 5.1 of the Berne Convention relies on the principle of national treatment. According to this principle, each member country must grant foreign authors (the nationals of other

---

<sup>82</sup> Weiskopf op cit note 10 at 7.

<sup>83</sup> Xalabarder op cit note 77 at 88.

<sup>84</sup> Idem at 80; Sterling op cit note 66 at 521-522.

<sup>85</sup> Sterling op cit note 66 at 520; David R. Johnson & David Post 'Law and Borders - The Rise of Cyberlaw' (1996) 48 *Stanford Law Review* 1367.

<sup>86</sup> Nimmer op cit note 53 at 5.

<sup>87</sup> For a complete discussion, see Xalabarder op cit note 77 at 88-94.

<sup>88</sup> Susan A Mort 'The WTO, WIPO & the Internet: Confounding the Borders of Copyright and Neighboring Rights' (1997) 8 *Fordham Intellectual Property, Media and Entertainment Law Journal* 173 at 216.

member countries) the same rights as it grants national authors. This does not solve the issue of what law should be applied when protection is sought for a country (or author) from a non-member country.<sup>90</sup> Article 5.2 of the Convention is a choice-of-law rule leading to the application of the law of the member country for which protection is claimed. However, online global information networks allow transmission to and access from servers in numerous countries. Article 5.2 does not solve the problem of infringements that take place in several countries simultaneously - does it imply that as many national copyright laws as countries into which the work may be received or accessed should be applied?<sup>91</sup> Or should national copyright laws be applied to acts that occur in other countries?<sup>92</sup>

The problems relating to deciding on an applicable law remain where a 'foreign element' is involved - where, for example, the person operating a web site is located in one country but at least part of the onward transmission process is carried out by people in other countries.<sup>93</sup>

Apart from the minimum standards set in international conventions, copyright legislation is still predominantly a national affair. So there are many variations in national copyright laws.<sup>94</sup> Until the advent of global information networks these differences between national copyright traditions could be tolerated. Where disputes involved cross-national conduct, there were choice-of-law rules, based largely on territorial considerations, with which to resolve the disputes. But cyberspace is not constrained by national boundaries. Because of their dependence on geographic considerations the existing conflict-of-law rules are inadequate to determine the applicable law in disputes arising in cyberspace.<sup>95</sup> The uncertainty about which national copyright rules should be applied can lead to a situation that an author may choose her jurisdiction based on the ground of which national law would be most beneficial to her

---

<sup>89</sup> Nimmer op cit note 53 at 7.

<sup>90</sup> Xalabarder op cit note 77 at 82.

<sup>91</sup> Idem at 83.

<sup>92</sup> Dixon & Hansen op cit note 10 at 607.

<sup>93</sup> Sterling op cit note 66 at 521-522.

<sup>94</sup> Thomas Dreier 'Unsolved copyright issues in the digital and network environment' (1995) 48 *Copyright World* 36 at 40; Gregory C Ludlow 'Copyright and the Challenge of the Digital World' (1999) 3 *Canadian International Lawyer* 199 at 205.

<sup>95</sup> Pamela Samuelson 'On Authors' Rights in Cyberspace: Questioning the Need for New International Rules on Authors' Rights in Cyberspace' accessible at <<http://www.firstmonday.dk/issues/issue4/samuelson/>> (visited on 21 November 2006) at 7.

claim.<sup>96</sup>

#### **2.3.3.4 The Enforcement of Judgments**

Even after an author obtained has judgment in her favour, it would often be virtually impossible to enforce the judgment against the infringer - in many instances the infringer is in a jurisdiction other than that of the author or the court that handed down judgment. Law enforcement depends on the ability to exercise physical control over, and impose sanction on, those who violate the law. A state can exercise such physical control only over subjects within its geographic borders. Infringers in cyberspace seldom find themselves within the geographic borders within which a state exercises control and impose sanctions.<sup>97</sup>

Even if it is possible to enforce the judgment, it would in many instances not be worth while. Usually the infringer is a private Internet user without sufficient economic resources to satisfy the judgment. So the effort and expense in locating and bringing action against the infringer will often not be justified.<sup>98</sup>

#### **2.3.4 Maintaining the Copyright Balance**

Copyright laws must strike a balance between protecting original works and providing sufficient incentive for authors to create original works, on the one hand, and protecting the public's rights of free expression, on the other hand. Over the years, copyright law, even in the Continental tradition, has evolved to represent a compromise and a balancing of interests among authors, publishers, and the public.<sup>99</sup> The law has also ensured the existence of a healthy public domain.<sup>100</sup> It is important to maintain this balance, since, as Justice Laddie<sup>101</sup> said, '[t]he whole of human development is derivative'. Overly protecting works would erode the public domain and so stifle the creation of new works.

---

<sup>96</sup> For a complete discussion of the problems relating to choice of law and jurisdiction in the digital world, as well as possible solutions, see Xalabarder op cit note 77 at 79-96.

<sup>97</sup> Johnson & Post op cit note 85 at 1368-1369.

<sup>98</sup> Weiskopf op cit note 10 at 7.

<sup>99</sup> Vinje op cit note 52 at 440.

<sup>100</sup> Idem at 436.

<sup>101</sup> Mr Justice Laddie 'Copyright: Over-strength, Over-regulated, Over-rated?' [1996] *European Intellectual*

Efforts to protect copyright in a digital environment can easily upset the balance between copyright rights and limitations.<sup>102</sup> The main focus in all discussions of this topic has been on the dangers to authors' rights. Often their rights have been stressed at the expense of the rights of users.<sup>103</sup> Emerging technologies to protect digital copyright works may actually also mean that author's rights will be better protected in cyberspace than they have ever been in the analogue world.<sup>104</sup> Considering this, the real difficulty when applying copyright law in cyberspace is to maintain the balance between incentives for creating and investing in works and the provision of adequate public access to works.<sup>105</sup>

Copyright in cyberspace has to be enforced in such way as to protect the rights of users<sup>106</sup> and to ensure the existence of a healthy public domain. Also, the rights of intermediaries in the digital world (like service providers and device manufacturers) have to be considered.

## 2.4 New Strategies for Protecting Copyright in the Digital Age

Technological progress creates an opportunity for economic prosperity. With this opportunity come numerous technical, financial, and legal challenges. By digitizing their works, authors expose it to misuse; and by publishing their works on the Internet, they lose control of the distribution of their works.<sup>107</sup> So the need arose for some kind of regulation or mechanism that would enable authors to exploit and control their works in digital format. If authors' rights are not properly protected, the success of the online global information networks can be compromised.<sup>108</sup> Although the security of the data flow over the Internet concerns not only

---

*Property Review* 253.

<sup>102</sup> J Litman 'Digital Copyright and Information Policy' accessible at <<http://www-personal.umich.edu/~7Ejdlitman/papers/casrip.html>> (visited on 21 November 2006) at 2.

<sup>103</sup> Bygrave op cit note 80 at 52; Simon Fitzpatrick 'Copyright Imbalance: U.S. and Australian Responses to the WIPO Digital Copyright Treaty' [2000] *European Intellectual Property Review* 214 at 217; Bowne op cit note 55 at 139; Sterling op cit note 66 at 520.

<sup>104</sup> Samuelson op cit note 95 at 9.

<sup>105</sup> Committee on Intellectual Property Rights and the Emerging Information Infrastructure; Computer Science and Telecommunications Board; Commission on Physical Sciences, Mathematics, and Applications; National Research Council op cit note 26 at 952; Fitzpatrick op cit note 103 at 217; Bowne op cit note 55 at 139; Sterling op cit note 66 at 520.

<sup>106</sup> Vinje op cit note 52 at 440.

<sup>107</sup> Kumik op cit note 11 at 21.

<sup>108</sup> Andre Lucas 'Copyright Law and Technical Protection Devices' (1997) 21 *Columbia - VLA Journal of Law and the Arts* 225.

authors but also government organizations,<sup>109</sup> online service providers,<sup>110</sup> and private individuals, I shall limit my discussion here to the protection of digital copyright digital works.

Authors' concerns about the threats posed by the digital revolution are unquestionably legitimate. But how should these concerns be addressed? Should it be left to authors to adopt measures to protect their works, or should new legal principles be drafted to regulate and protect digital copyright works? Or is a combination of these the answer?

Barrow<sup>111</sup> offers 'rights clearance' as the solution. He argues that rights clearance is 'perhaps the single most important requirement for the economic exploitation of the "information superhighway". . .' An effective rights clearance system will ensure not only that copyright works transmitted digitally will earn a fair return for their owners but also that users will benefit from the wider and faster availability of new and existing works.

Marks and Turnbull,<sup>112</sup> however, believe that 'right clearance' can be effective only if it is implemented on three levels - by authors, through negotiated cross-industry agreements and licences, and by new legislative provisions.

#### **2.4.1 Strategies employed by Authors to Protect Their Works**

Authors can use two strategies to exploit and control their works in digital format - contractual conditions, and technological protections.<sup>113</sup>

---

<sup>109</sup> Encryption has especially been a tool in the conduct of military and foreign affairs. See David Flint 'Encryption - Plainly Free Speech?' (2000) 102 *Copyright World* 19.

<sup>110</sup> Online service providers are concerned with the security of data flows, not because they are concerned about the protection of the data itself, but because they are concerned about retaining customers and to avoid losing their investment.

<sup>111</sup> Edward Barrow 'Rights clearance and technical protection in an electronic environment' accessible at <<http://associnst.ox.ac.uk/~icsuinfo/barrow.htm>> (visited on 20 March 2002) at 1.

<sup>112</sup> Marks & Turnbull op cit note 2 at 198.

<sup>113</sup> William Cornish & David Llewellyn *Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights* 5 ed (2003) § 13-87. Barrow op cit note 111 at 3-4 identifies two additional rights clearance systems available to content owners, namely copyright accounting and settlement systems and copyright management systems. Copyright Accounting and Settlement Systems basically provides for billing and settlement procedures, and by making it quick and simple to make a payment, prevent unauthorized copying. The function of an Electronic Copyright Management System (ECMS) is to manage legitimate uses of material. It ensures that the legitimate user accessed the material and that accesses were properly recorded, so that the rights-holder

### 2.4.1.1 Contractual Conditions

An author can protect and control her works by means of contractual conditions. Agreements to conditions of use can be concluded through ‘shrink-wrap’ and ‘click-wrap’ contracts.<sup>114</sup> It is mainly used by software developers and publishers and is usually in the form of a licence agreement.<sup>115</sup>

In the case of a ‘shrink-wrap’ contract, a printed standard-form agreement is affixed to the surface of the packaging of computer software and sealed in a plastic or cellophane wrapper. By opening the package the purchaser accepts the offer made on the standard-form agreement and a valid contract, separate from the contract of sale, arises.<sup>116</sup> Failure to fulfil the conditions on the standard-form agreement amounts to breach of contract.

In the case of a ‘click-wrap’ agreement, the person seeking access to the content must agree to accept (by ‘click-on’) the contractual offer displayed on the computer screen before she will be able to gain access to the material. The offer made by the author will usually be in standard form - take it or leave it.<sup>117</sup> After acceptance of the offer, a contract arises and the user who copies or distributes the content contrary to these contractual conditions is liable for breach of contract.<sup>118</sup>

The practice of using ‘shrink-wrap’ and ‘click-wrap’ agreements has been legitimized in the United States of America in *ProCD Inc v Zeidenberg*.<sup>119</sup> It has been held that these agreements are generally enforceable, despite invalidation for public policy reasons, if notice

---

could be fairly rewarded.

<sup>114</sup> ‘Digital technology and the Copyright Act 1994: A Discussion Paper - Part Two: Background’ op cit note 8.

<sup>115</sup> Stephen J Davidson, Scott J Berg & Michael Kapsner ‘Open, Click, Download, Send - To What Have You Agreed?’ (2001) 4 *Journal of Internet Law* 1 at 5.

<sup>116</sup> Davidson, Berg & Kapsner op cit note 115 at 6; OH Dean *Handbook of South African Copyright Law* (loose-leaf, revision service 12, 2004) 1-86 - 1-87; Fleischmann op cit note 6 at 21; Michael Landau ‘Digital Downloads, Copy Code, and U.S. Copyright Law’ *9th Annual Conference on Intellectual Property Law and Policy, New York, 19 April 2001*, 1 at 21; and T Pistorius ‘The Enforceability of Shrink Wrap Agreements in South Africa’ (1993) 5 *South African Mercantile Law Journal* 1 at 3-10, 19.

<sup>117</sup> Cornish op cit note 113 § 13-87.

<sup>118</sup> Davidson, Berg & Kapsner op cit note 115 at 7.

<sup>119</sup> 86 F 3d 1447 (7th Cir. 1996).

is provided and an opportunity to return the product is given.<sup>120</sup>

Vinje<sup>121</sup> identifies the following danger of contractual protection in the digital context. There, authors have the ability to contract directly with users. This could encourage authors to restrict acts by contract that they would not have been able to restrict through copyright. In some instances, contractual restrictions that exceed the scope of copyright may be rendered unenforceable through the application of non-copyright doctrines such as the abuse of rights, or of competition or consumer-protection laws. But, according to Vinje, it is unlikely that the results of applying non-copyright doctrines will reflect the balance contained in copyright law. He then raises the question - to what extent may copyright exceptions limit the ability to enforce such contractual restrictions? So the question is whether contract law is subject to copyright limits and exceptions.

It seems as if Vinje's objections to contractual protections in the digital environment are not unfounded. In the United States, an attempt was made to validate contracts favouring software vendors (who, in many instances, would also be the authors). In December 1998, a new article 2B of the Uniform Commercial Code,<sup>122</sup> on electronic contracting, was proposed. Article 2B of the UCC was then replaced with the Uniform Computer Information Transactions Act (UCITA),<sup>123</sup> a draft state law for contracts relating to software and other forms of computer information. The UCITA was submitted in 1999 as a proposed Uniform Act by the Uniform Law Commissioners. UCITA represents a movement toward licensing of information in its many forms and away from the sale of copies as traditionally understood under copyright law. UCITA would enforce the broad use of "shrink-wrap" and computer "click-on" licenses (called "mass-market licenses" in UCITA). By licensing rather than selling something, a vendor can wield more control of the downstream use of the product. It therefore shifts the balance of existing contract law in favour of software vendors (authors) when they contract with consumers (users). The UCITA was extremely controversial and as a

---

<sup>120</sup> Jason Sheets 'Copyright Misused: The Impact of the DMCA Anti-circumvention Measures on Fair & Innovative Markets' (2000) 23 *Hastings Communications and Entertainment Law Journal* 1 at 6 note 18 and accompanying text.

<sup>121</sup> Thomas Vinje 'Copyright Imperilled?' [1999] *European Intellectual Property Review* 192-207 at 195.

<sup>122</sup> UCC § 2B-105(a) and § 2B-105(b).

<sup>123</sup> The Uniform Computer Information Transactions Act 1999: Draft for Approval accessible at <<http://www.law.upenn.edu/bll/ulc/ucita/citam99.htm>> (visited on 20 November 2006).

result was withdrawn in 2002. Because of the opposition, UCITA has been passed only in two states - Virginia, and Maryland. Despite the fact that it has not been passed extensively as state law, UCITA indicates to what extent contract law can potentially shift the copyright balance in favour of authors.<sup>124</sup>

Unfortunately UCITA is not the only example of legislative measures that provide that contractual agreements override established copyright exceptions. This can also be seen from article 6.4(1) and (4) of the EC Directive on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society.<sup>125</sup> Article 6.4(1) encourages voluntary agreements between authors and users with regard to those seven exceptions in national law safeguarded in this subparagraph, whereas article 6.4(4) allows authors to contract out of copyright exceptions when they provide interactive on-demand services. Article 9 of the Directive also expressly states that '[t]his Directive shall be without prejudice to provisions concerning in particular . . . the law of contract'.<sup>126</sup>

Contractual conditions need not be used independently as protection measures. They can also be used in conjunction with technological protection measures. It can, for example, be a condition for the supply of any material that it may be used only in association with a specified technological protection system.<sup>127</sup> Failure to fulfil this condition amounts to breach of contract.

#### **2.4.1.2 Technological Protection**

Many authors believe that the same technology that threatens copyright may also be used to

---

<sup>124</sup> See, inter alia, <[http://civies.com/content/agents/2b\\_agent.htm](http://civies.com/content/agents/2b_agent.htm)> visited on 28-02-2005; A Quick look at the Uniform Computer Information Transactions Act accessible at <<http://www.arl.org/info/frn/copy/ucita.html>> (visited on 21-11-2006);

<[http://www.bambooweb.com/articles/u/n/Uniform\\_Computer\\_Information\\_Transactions\\_Act.html](http://www.bambooweb.com/articles/u/n/Uniform_Computer_Information_Transactions_Act.html)> visited on 28-02-2005; and UCITA: Uniform Computer Information Transactions Act accessible at <<http://www.jameshuggins.com/h/tek1/ucita.htm>> (visited on 21 November 2006).

<sup>125</sup> Directive 2001/29/EC of the European Parliament and the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society accessible at <[http://europa.eu.int/documents/comm/index\\_en.htm](http://europa.eu.int/documents/comm/index_en.htm)> (visited on 21 November 2006).

<sup>126</sup> Alvise Maria Casellati 'The Evolution of Article 6.4 of the European Information Society Copyright Directive' (2001) 24 *Columbia-VLA Journal of Law & The Arts* 369 at 392.

<sup>127</sup> Barrow op cit note 111 at 3 and 'Digital technology and the Copyright Act 1994: A Discussion Paper - Part Two: Background' op cit note 8.

protect copyright works.<sup>128</sup> Since digital technology can be used to trace, monitor, and control the reproduction and dissemination of works,<sup>129</sup> it can be successfully employed to protect copyright works. Whilst copyright law can be applied only after infringement has occurred, as it does not work prospectively,<sup>130</sup> technological protection measures work prospectively and can effectively *prevent* infringement. Also, while copyright law provides authors merely with a *right* to control the use of their copyright works, technological protection measures enable authors to exercise *factual control* over what users can and cannot do with their works.<sup>131</sup> Accordingly, as Clark<sup>132</sup> so aptly stated, many authors believe that ‘[t]he Answer to the Machine is in the Machine’.

Technological protection comes in many shapes and can be categorized in different ways.<sup>133</sup> For purposes of this discussion I will follow the two broad categories as found in the WIPO Copyright Treaty - technological protection measures,<sup>134</sup> and rights management information.<sup>135</sup> Technological protection measures control access to, or the use of copyright works, and so restricts a user’s freedom of ‘movement’.<sup>136</sup> Rights management information administers the rights of authors and places the pertinent information under safekeeping.<sup>137</sup>

#### **2.4.1.2.1 Technological Protection Measures**

---

<sup>128</sup> See, inter alia, David Price ‘Fighting Fire with Fire: Monitoring Intellectual Property in a Digital Age’ (2001) 111 *Copyright World* 14-15; Lucas op cit note 108 at 226; and Vinje op cit note 52 at 431-440.

<sup>129</sup> Green Paper on Copyright and Related Rights in the Information Society, Commission of the European Communities, COM(95) 382 final, 19 July 1995, at 49 to 50.

<sup>130</sup> Casellati op cit note 126 at 371.

<sup>131</sup> Kamiel J Koelman ‘A Hard Nut to Crack: The Protection of Technological Measures’ [2000] *European Intellectual Property Review* 272.

<sup>132</sup> Charles Clark ‘The Answer to the Machine Is in the Machine’ in P Bernt Hugenholtz (ed.) *The Future of Copyright in a Digital Environment* (1996) 139-146.

<sup>133</sup> See Institute of Information Law, Amsterdam ‘Protection of Technological Measures’ November 1998 accessible at <<http://www.imprimatur.net/IMP-FTP/technical.pdf>> (visited on 27 June 2002) at 2 footnote 1 for several classification systems. In this document four categories are listed, but, as will be seen later, these four categories are basically only subdivisions of the two broad categories into which these measures are divided by the WCT. Price op cit note 128 at 15 also mentions a Discovery Engine (developed by Envisional) that trawls through every part of Internet and can be used to monitor - and take action against - websites that are illegally posting music files on the Internet.

<sup>134</sup> Article 11 of the WIPO Copyright Treaty. Nick Hanbidge ‘DRM: Can It Deliver?’ (2001) 12 *Entertainment Law Review* 138 refers to this as a method of ‘secure distribution’.

<sup>135</sup> Article 12 of the WIPO Copyright Treaty. Hanbidge op cit note 134 refers to this as a method of ‘digital watermarking’.

<sup>136</sup> Lucas op cit note 108 at 227.

<sup>137</sup> Bygrave op cit note 80 at 52 states that rights management information identifies a product as well as the person who owns the copyright therein and ensures that the latter identification data are authentic. See also Lucas op cit note 108 at 227.

The aim of technological protection measures is to protect or secure works in digital format. It can be integrated in software or built into the hardware.<sup>138</sup> Hanbidge<sup>139</sup> refers to this type of technology as a method of ‘secure distribution’.<sup>140</sup> Secure distribution relies upon encryption, which is the starting point for an infinite number of applications.<sup>141</sup> Encryption is the key element to distinguish between authorized and unauthorized uses, since no individual or device can decrypt content ‘by accident’.<sup>142</sup>

Encryption<sup>143</sup> entails the digital scrambling of the bits that make up the work so that the work cannot be accessed or clearly seen. In order to access or use the work, one needs a ‘key’ (a magic number that is used to descramble (decrypt) the original work).<sup>144</sup> The key is issued only to authorized users, either for payment or after confirmation that the user is indeed authorized to access or use the work.<sup>145</sup>

Although encryption is presently the only technology that prevents the first unauthorized use, it is not infallible.

In the first instance, after decryption (whether by means of an authorized key or through hacking) the work is vulnerable to abuse. A decrypted work can be accessed and used by anyone. Encryption also does not protect the integrity of a work - material can be decrypted, altered, and then re-encrypted using the same key.<sup>146</sup>

---

<sup>138</sup> Committee on Intellectual Property Rights and the Emerging Information Infrastructure; Computer Science and Telecommunications Board; Commission on Physical Sciences, Mathematics, and Applications; National Research Council op cit note 26 at 962-963; Lucas op cit note 108 at 226.

<sup>139</sup> Hanbidge op cit note 134 at 138.

<sup>140</sup> Secure distribution is nothing other than a form of cryptography, the science of keeping information secret. Although it was initially exclusively used by Government organizations, the advent of Internet lead to a demand for security of all data flows, and cryptography became the method how this demand can be met. The power to keep secrets now vests in any person equipped with a personal computer and the relevant software who wishes to keep his communications confidential or to effect a secure electronic transaction. Flint op cit note 109 at 19 and Gabriela Kennedy ‘Encryption Policies: Codemakers, Codebreakers and Rulemakers: Dilemmas in Current Encryption Policies’ (2000) 16 *Computer Law & Security Report* 240 at 240-241.

<sup>141</sup> Hanbidge op cit note 134 at 138; Lucas op cit note 108 at 226.

<sup>142</sup> Marks & Turnbull op cit note 2 at 204.

<sup>143</sup> This is sometimes referred to as wrapping or enveloping, but it is essentially an encryption process: see Marks & Turnbull op cit note 2 at 212.

<sup>144</sup> Kumik op cit note 11 at 21-22; Flint op cit note 109 at 19; and Barrow op cit note 111 at 5.

<sup>145</sup> Barrow op cit note 111 at 5; Marks & Turnbull op cit note 2 at 212.

<sup>146</sup> Barrow op cit note 111 at 5-6.

Secondly, the encryption/decryption process can overload on machine time. Sometimes this will unacceptably slow down the operation. Although this problem is likely to be resolved by the growth in processor power, it makes encryption more vulnerable to the brute force attack of trying every possible combination.<sup>147</sup>

Since technological protection measures are used to control either access to or the use of copyright works, two types of technological protection measure have emerged - access control, and copy control.

#### **2.4.1.2.1.1 Access Control**

The most basic and important type of technological protection is access-control technology: it prevents someone from viewing, reading, hearing, and/or otherwise perceiving the work without the author's consent.<sup>148</sup> It can either prevent access at the online outlet or at the level of the user of the information, or can be used to control or prevent subsequent access to an already acquired copy of a work.<sup>149</sup> An access measure can protect a service as well as the content provided by that service. Measures that control access to an already acquired work differ from those that prevent access at the online outlet or at the receiver end in so far as they control access only to the work itself and not to any service.<sup>150</sup>

When used as an access control, encryption effectively 'locks' digital works to ensure that only authorized users have the keys to unlock and use it.<sup>151</sup> Encryption is, however, not the only method used in access control technologies. Access may also be conditional upon passwords or other means of data authentication.<sup>152</sup>

At least three different forms of access control can be distinguished:

---

<sup>147</sup> Idem at 5.

<sup>148</sup> June M Besek 'Anti-Circumvention Laws and Copyright: A Report from the Kernochan Center for Law, Media and the Arts' (2004) 27 *Columbia Journal of Law & the Arts* 385 at 450.

<sup>149</sup> Vinje op cit note 121 at 196; Institute of Information Law op cit note 133 at 2-3.

<sup>150</sup> Vinje op cit note 121 at 196-197.

<sup>151</sup> David Fletcher 'Brave New eWorld - What Lessons can the ePublishing Industry Learn from the Music Industry?' (2000) 105 *Copyright World* 9 at 10.

#### **2.4.1.2.1.1.1 Initial Access Control**

The first type of access control controls access to a copy or a performance at the online outlet such as the web site of an information provider.<sup>153</sup> The access control measure can take the form of a password, in which the user must provide identification, often a unique password, in order to access the protected work. Examples of this type of protection are the passwords necessary to access the LexisNexis or Westlaw databases.<sup>154</sup>

We can compare an initial access control measure to the access control applied by a bookshop or a movie theatre. A difference is, of course, that in the case of the latter case actors mostly do not know the identities of their customers, whereas many web-site operators require the submission of personal data before access is granted. This raises privacy and data-protection issues - is it desirable that the data on which a person gained access be processed and made available?<sup>155</sup>

#### **2.4.1.2.1.1.2 Receiver-end Access Control**

The second species of access control has a similar function but is implemented at the receiver end. It is, therefore, exercised in the user's private sphere. Examples of receiver-end access controls are decoders or set-top boxes. These measures can be regarded as protecting a service (like pay television) as well as the content provided by that service.<sup>156</sup>

#### **2.4.1.2.1.1.3 Subsequent Access Control**

The third type of access control does not only concern initial access but also each subsequent act of access or consultation even of a purchased or downloaded copy.<sup>157</sup>

---

<sup>152</sup> Lucas op cit note 108 at 227.

<sup>153</sup> Koelman op cit note 131 at 276; Vinje op cit note 121 at 196.

<sup>154</sup> Besek op cit note 148 at 450.

<sup>155</sup> Koelman op cit note 131 at 276.

<sup>156</sup> Vinje op cit note 121 at 196.

<sup>157</sup> Koelman op cit note 131 at 276.

This type of access control enables new modes of exploitation. It is expected that in the digital era information will be consumed on a pay-per-use, rather than a pay-per-copy, basis. Consumers will purchase a copy that will disintegrate after a certain period or when it has been played a certain number of times. Pay television already applies an accounting scheme based on individual initial access but until now it has not prevented consumers from copying the programme or sharing the copy. New technologies facilitate billing for such subsequent uses.<sup>158</sup>

Besek<sup>159</sup> refers to Movielink as an example of an access control. Movielink is an online movie 'rental' service that allows a user, against payment, to download a movie to her computer for viewing. The user then has 30 days to watch the movie. However, once the user accesses it, she will be able to access it only for 24 more hours, after which the movie deletes itself from her hard drive.<sup>160</sup>

Advocates of these new business models proclaim that an advantage is that the author will be able to reap the full value of any use of her work, which in their view is the main purpose of copyright. At the same time consumers will pay only for the value that they actually extract from the work. If, for example, they play a musical work three times, they will be billed only for those three times, instead of buying a (copy of a) work at a price that is presumably predicated upon unlimited access.<sup>161</sup>

#### **2.4.1.2.1.2 Copy Control**

By controlling access one can control use of a work generally - if a work cannot be accessed, it cannot be used. However, sometimes an author wants to give access to her work while controlling subsequent uses. In order to do so, the author can employ copy or use controls.

---

<sup>158</sup> Idem at note 34 refers to the DIVX (Digital Video Express) standard that was introduced in the United States. DIVX was a DVD format, allowing the purchaser to view the disk for only two days after it was first accessed. After this time period, it could be used as a pay-per-view feature, or just be thrown away. The dedicated DIVX players included a modem and would send billing information over the phone line every time the copy was viewed after the first two days. The idea was for the DIVX to replace the video rental market. The DIVX project has been terminated for several reasons. See <http://bsuvc.bsu.edu/jrfoust/techno.html>.

<sup>159</sup> Besek op cit note 148 at 450.

<sup>160</sup> Ibid.

<sup>161</sup> Koelman op cit note 131 at p 276.

Copy control enables the author to limit the user's freedom of movement once she has accessed the work. It thus allows authorized activities but prevents unauthorized activities by the user who already accessed the work.<sup>162</sup> Copy control technology limits whether and to what extent a work can be copied, communicated, viewed, or played.<sup>163</sup>

Copy protection is the predominant function of this type of technological protection measure. Copy controls prevent or limit copying, or, more generally, limit the kinds of uses that may be made of a work. When used as a copy control, encryption makes content files unreadable once they have been copied so that the content is of no value to the recipient of the copied file.<sup>164</sup>

A widely-implemented copy control is the Serial Copyright Management System (SCMS). This system prevents the making of digital copies of a digital copy. In other words, SCMS allows one copy to be made of a work but prevents copies being made of that copy, so that it cannot be used as a 'digital master'.

Other measures prevent making any copies of digital works. An example of such a system is the Copy Generation Management System (CGMS), an agreed standard that controls the copying of DVD video, which can be calibrated to prevent entirely the making of any digital copies.<sup>165</sup>

Other methods include planting a 'worm' in computer programs, which detects efforts to copy the program and 'counterattacks' by erasing the copied files. A product may also be designed to prevent the making of print-outs or copies of the product in its entirety, by blocking these functions through software routines.<sup>166</sup>

Access controls and copy controls often overlap. Once a copy control key is stripped out,

---

<sup>162</sup> Lucas op cit note 108 at 227.

<sup>163</sup> Besek op cit note 148 at 450.

<sup>164</sup> Institute of Information Law op cit note 133 at 3.

<sup>165</sup> Vinje op cit note 121 at 197.

<sup>166</sup> These and other copy protection mechanisms were widely used in connection with computer software in the 1980s, but because consumers resented the inconvenience and the mechanisms were easy to break, copy-protection technologies are no longer popular (Institute of Information Law op cit note 133 at 3).

everyone has access to the work without the author's consent - the copy control can accordingly also control access to a work.<sup>167</sup> The Content Scramble System (CSS) is an example of a technology that serves as both an access control and a copy control. Motion picture studios use CSS to encrypt DVD contents. Since only licensed devices can decrypt and play CSS-protected DVDs (thus granting the user access to the contents). CSS serves as access control, and since it generally also prohibits copies being made of the contents of the DVD, it serves as copy control.

#### **2.4.1.2.2 Rights Management Information**

Technological protection measures protect works only against unauthorized access or uses. They do not ensure the integrity of works, or provide a system by which authors can control their works once they have been accessed. Rights management information,<sup>168</sup> therefore, is the next logical step after the implementation of a technological protection measure. It 'hides information' in digital files,<sup>169</sup> which information identifies the work and makes it possible to track the uses and automate the administration of the rights relating to such uses.<sup>170</sup>

Unlike technological protection measures, rights management information barely intrudes on the user's experience. In fact, the user will not even know that the work she is accessing has been digitally marked. Rights management information is embedded in the content file and travels with it throughout its journey in cyberspace so that the author can trace it by using specific software that can decipher the mark.<sup>171</sup>

---

<sup>167</sup> 'Panel III: Implications of Enforcing the Digital Millennium Copyright Act: A Case Study, Focussing on United States v. Sklyarov' (2002) 12 *Fordham Intellectual Property, Media and Entertainment Law Journal* 805 at 834-835.

<sup>168</sup> Article 12 of the WCT defines 'rights management information' as 'information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public.'

<sup>169</sup> It is therefore nothing other than a method of steganography. (Steganography refers to methods of hiding information in other data such as visual images, voice communications and music.)

<sup>170</sup> The first part of the Agreed Statement adopted by the Diplomatic Conference concerning Article 12 of the WCT reads as follows: 'It is understood that the reference to "infringement of any right covered by this Treaty or the Berne Convention" includes both exclusive rights and rights of remuneration.' Article 12 of the WCT deals with the protection of rights management information. The Treaty thus makes provision that rights management information can be applied to protect not only exclusive rights, but also remuneration rights. See also Fitzpatrick op cit note 103 at 222 and Lucas op cit note 108 at 229.

<sup>171</sup> Hanbidge op cit note 134 at 138.

Rights management information provides a passive form of defence. Although it cannot prevent unauthorized copying or distribution, it enables owners to monitor uses of their works. Rights management information has several uses: it provides forensic evidence of authorship;<sup>172</sup> it advances moral rights;<sup>173</sup> it enables authors to maintain an audit trail, keeping them better informed about who is using their content, when, and in what context;<sup>174</sup> it can be used to trace the source of infringing material amongst other licensed material;<sup>175</sup> and it is used to channel payments digitally to the appropriate authors.<sup>176</sup> It facilitates the publishing of digital content on the Internet, since it allows authors to protect their rights.<sup>177</sup>

Rights management information can be divided into two categories, depending on its functions – authenticity and integrity protection, and usage metering.<sup>178</sup>

#### **2.4.1.2.2.1 Authenticity and Integrity Protection**

Rights management information can also be used to verify the authenticity of a work (whether it is actually the work of the author whose work it claims to be), and its integrity (whether any alterations to the work have been made, whether purposely or inadvertently).<sup>179</sup>

In the context of copyright law, the authenticity of a work relates to the author's paternity and integrity rights. So rights management information has the potential to play a very important role in the protection of an author's moral rights. But it would also play an important role in the protection of economic rights, since the value of a work is often determined by the

---

<sup>172</sup> Derrick Grover 'Data Watermarking: Steganography and Watermarking of Digital Data' (2001) 17 *Computer Law & Security Report* 101.

<sup>173</sup> A digital signature could, for instance, guarantee that the rights of paternity and integrity be properly exercised. Lucas op cit note 108 at 231.

<sup>174</sup> Fletcher op cit note 151 at 10.

<sup>175</sup> Grover op cit note 172 at 101.

<sup>176</sup> The first part of the Agreed Statement adopted by the Diplomatic Conference concerning Article 12 of the WCT reads as follows: 'It is understood that the reference to "infringement of any right covered by this Treaty or the Berne Convention" includes both exclusive rights and rights of remuneration.' See also Fitzpatrick op cit note 103 at 222.

<sup>177</sup> Kumik op cit note 11 at 21.

<sup>178</sup> See contra Besek op cit note 148 at 450-453 who sees integrity and authenticity controls, as well as tracking controls (metering systems) as subspecies of technological protection measures, and not as types of rights management information.

<sup>179</sup> *Idem* at 450.

identity of its author. Furthermore, a work would lose its value if users know or believe that it has been altered.

When used for integrity protection, rights management information prevents a work from being altered.<sup>180</sup> Integrity protecting technologies are not yet widely used in the context of copyright protection. Until now, the issue of the integrity of electronic information has mainly been addressed as a problem of authentication - to what extent does an electronic document or signature constitutes valid proof of a transaction?<sup>181</sup>

Watermarking ('tattooing') is a technique used to verify the authenticity of a work and to protect the integrity of a work. A watermark is an embedded copyright message that can provide information about the author (to identify the author), rights, distribution, and so on. It can also contain copy control information and instructions.<sup>182</sup> So it has a role to play in providing evidence.<sup>183</sup>

Watermarking involves the creation of a permanent, indelible mark in the digital record. Bits are embedded into the work that cannot audibly or visually be detected. They can, however, be read by a detection device so that a user can detect whether the work is authentic, and where the work originated. Watermarks appear as random information or 'digital noise' in the work and are almost impossible to identify and extract.<sup>184</sup>

A watermark can be effective only if compliant directors that read and respond to the watermark are embodied in the playback and recording devices; if not, the watermark will pass undetected. One of the difficulties with a watermark is that it must survive compression methods without becoming visible or audible when uncompressed.<sup>185</sup>

Very compact file formats cannot be watermarked, as watermarking requires some data

---

<sup>180</sup> Institute of Information Law op cit note 133 at 4.

<sup>181</sup> Ibid.

<sup>182</sup> Marks & Turnbull op cit note 2 at 212.

<sup>183</sup> Grover op cit note 172 at 102.

<sup>184</sup> Bowne op cit note 55 at 144-145.

<sup>185</sup> Marks & Turnbull op cit note 2 at 212.

redundancy in the file to accommodate it.<sup>186</sup>

#### **2.4.1.2.2 Usage Metering**

The second main category of rights management information is usage metering. It facilitates the exploitation of a work since it can be used to track the frequency with which a work is accessed, or to monitor the uses made of the work. The next step in the development of usage metering would be the automatic and simultaneous online payment for each use.<sup>187</sup>

Fingerprinting is the technique used to identify and monitor the receipt and use of digital works.<sup>188</sup> It is an extension of watermarking.<sup>189</sup> As well as the mark identifying the work (the watermark), a mark identifying the user or the user's system is included by the user's system at the time of use. This allows the author to charge the fee to the right person, and it creates an identifying trail to trace the source of infringing copies.<sup>190</sup> An example of a fingerprint is a 'webcrawler', which is a program that methodically searches the Internet for copies of specified material and report where and when they were found. The recording industry, in particular, uses webcrawlers to detect unauthorized copies of sound recordings and also to meter usage for licensing purposes.<sup>191</sup>

### **4.1.3 Inadequacy of Strategies Employed by Authors**

Contractual and technological protections have an important role to play in protecting the authors' interests in their digital works.<sup>192</sup> But contractual conditions can be enforced only against parties to the agreement, and technological protection consists of two imperfect technologies. Rights management information can track but not prevent unauthorized copying. Technological protection measures can prevent unauthorized copying but is

---

<sup>186</sup> Barrow op cit note 111 at 6.

<sup>187</sup> Institute of Information Law op cit note 133 at 4.

<sup>188</sup> Bowne op cit note 55 at 145.

<sup>189</sup> Grover op cit note 172 at 102.

<sup>190</sup> Ibid.

<sup>191</sup> Besek op cit note 148 at 451.

<sup>192</sup> Nick Hanbidge 'Protecting Rights Holders' Interests in the Information Society: Anti-circumvention; Threats Post-Napster; and DRM' (2001) 12 *Entertainment Law Review* 223 at 225.

vulnerable to hacking.<sup>193</sup> Even when technological protection measures are combined with rights management information, they are, for the following reasons, insufficient to provide adequate protection for copyright works.<sup>194</sup>

In the first instance, technological protection measures can be hacked. Circumvention devices threaten the integrity of technological protection measures, and unauthorized passwords and access codes frustrate access controls.<sup>195</sup> No technological measure can permanently resist deliberate attacks by hackers and so cannot prevent piracy.<sup>196</sup> It rather serves ‘to keep honest people honest’ and poses an obstacle to those who seek to violate the measure. Breach of contractual conditions entitles authors to contractual remedies, but what remedies are at their disposal for the circumvention of their technological protection measures?

Secondly, authors depend on wide audiences of legitimate, paying users to support the creation and distribution of their works. Authors reap economic value by having their works seen, heard, and read by users. So protection technology must not interfere with the legitimate distribution to and communication of their works to the public. It should prevent only illegitimate uses. This means that copy-protection measures cannot be unilateral. Authors cannot apply protection measures to their works that will render all receiving and playback devices unable to receive or play their works. Therefore, in order to work properly, the copy protection technologies applied by authors need to function with consumer electronics and the computer devices used by consumers. These devices, in turn, need to respect and respond to the technologies applied by authors. So effective copy protection requires agreement between and implementation by both authors and the manufacturers of consumer electronics and computer products.<sup>197</sup>

Thirdly, the implementation of protection technologies can be limited severely by the problem of an already existing and installed base of consumer devices that cannot function

---

<sup>193</sup> Hanbidge op cit note 134 at 140.

<sup>194</sup> Marks & Turnbull op cit note 2 at 199.

<sup>195</sup> Vinje op cit note 52 at 431.

<sup>196</sup> <<http://www.ifpi.org/site-content/library/wipo%20treaties%20-%20technical%20measures.pdf>> on 5/4/2002 ; Marks & Turnbull op cit note 2 at 199.

<sup>197</sup> Marks & Turnbull op cit note 2 at 199-200.

with such technologies.<sup>198</sup>

Fourthly, technology cannot retroactively protect works that are already available in the marketplace without technological protection.<sup>199</sup>

Fifthly, it is unlikely that technological protection will be implemented in all environments and with respect to all formats. So strong legal regimes backed up by effective enforcement and remedies remain indispensable.<sup>200</sup>

It is clear that effective protection of works in the digital environment require a combination of three fields of protection - protection (especially technological protection) applied by authors, negotiated cross-industry agreements, and legal protection.

#### **2.4.2 The Need for Negotiated Cross-Industry Agreements and Licences**

Effective copy protection requires agreement and implementation by both authors and manufacturers of consumer electronics and computer products.<sup>201</sup> Only protection devices unanimously approved by all interested parties are destined for any future use.<sup>202</sup> Authors, the consumer electronics industry, the computer industry, the broadcast industry, and the telecommunications industry need to work together to develop and implement protection technologies and rules for content use.<sup>203</sup> Cross-industry agreements and structures in terms of which technological protection measures are established through the use of commercial licensing arrangements are indispensable.<sup>204</sup>

---

<sup>198</sup> *Idem* at 200.

<sup>199</sup> *Ibid.*

<sup>200</sup> *Ibid.*

<sup>201</sup> *Idem* at 199-200.

<sup>202</sup> Lucas *op cit* note 108 at 228.

<sup>203</sup> Marks & Turnbull *op cit* note 2 at 203.

<sup>204</sup> An example of such an agreement is the Content Scrambling System ('CSS') License Agreement. CSS is an encryption system for DVDs developed jointly by Matsushita Electrical Industrial Co. and Toshiba Corporation. Matsushita and Toshiba licensed CSS to the DVD Copy Control Association (the 'DVD-CCA') for purposes of administering CSS and licensing the technology. If a manufacturer wants a CSS decryption 'key', it must agree to the terms of the DVD-CCA licence and pay certain fees to the DVD-CCA. The terms of the licence are determined by the members of the DVD-CCA, and its membership includes all of the major motion picture studios. The motion picture studios would not have released their content encrypted with CSS unless they could be sure it was protected, and the DVD-CSS licence accomplishes that. CSS alone is not a very powerful encryption system - its power lies in the fact that it is supported by licenses and the law. See Kramarsky *op cit*

Different goals and principles provide guidelines on how to reach these agreements and establish these structures. General principles that guide current protection efforts include the principles that participation in copy-protection structures should be voluntary,<sup>205</sup> that content should be encrypted,<sup>206</sup> that copy-protection rules should be imposed by encryption and/or decryption licences,<sup>207</sup> that these technologies should be applied to devices and systems,<sup>208</sup> that recording and playback should be controlled,<sup>209</sup> that technologies should be made available on reasonable and non-discriminatory terms,<sup>210</sup> and that meaningful protection should be sustained.<sup>211</sup>

However, the transformation of these goals and principles into actual copy-protection systems is not easy.<sup>212</sup> Innovation of protection technologies is an ongoing process that requires research and development, and the implementation of protection technologies requires co-operation across industries.

---

note 5 at 10-12.

<sup>205</sup> Both authors as well as device manufacturers should have a choice whether they want to participate in a copy protection structure or not. There is, however, an obligation on device manufacturers: if they decide not to participate, then their products must neither circumvent nor interfere with copy protection technology used by authors (see Marks & Turnbull *op cit* note 2 at 203-204).

<sup>206</sup> Encryption of content is the key to distinguish between authorized and unauthorized uses. No individual or device can decrypt content 'by accident'. Encryption of content is therefore the keystone of current copy protection efforts. See Marks and Turnbull *op cit* note 2 at 204.

<sup>207</sup> *Ibid.* The encryption and decryption of content requires a licence of the relevant encryption technology. This licence will include obligations concerning what copy protection rules must be followed (eg no copies allowed, one copy allowed, etc) as a condition for decrypting the content and making it accessible to the user. Ideally, content should be watermarked with the copy protection rules and terms of use of the content. Any unlicensed device may transmit or pass on encrypted content without restrictions, provided that such a device does not decrypt or otherwise make the content accessible. Any unlicensed device that decrypts the content violates anti-circumvention law (as well as any proprietary rights of the owners of the encryption technology).

<sup>208</sup> *Ibid.* Copy protection technology and obligations should be applied to all devices and services that are capable of playing back, recording and/or transmitting protected content. All devices and delivery systems must therefore maintain content as securely as it was received and neither circumvent protections nor release content to the next device or component in the clear. This means that such devices and systems may not pass content which has been legitimately decrypted to other devices and systems without the appropriate protections.

<sup>209</sup> *Ibid.* Recording devices should read and respond to watermarks and refuse to copy content that is marked 'no copy'. Devices and systems should therefore not read back (ie play or display) content that is watermarked as 'no copy'. Similarly, there should be no read back from any copy of content that is marked 'copy once' beyond the single authorized copy.

<sup>210</sup> *Ibid.* Technical protection measures should be made widely available on fair and non-discriminatory terms for implementation by all relevant parties (such as authors and manufacturers).

<sup>211</sup> Copy protection systems and technologies need to provide meaningful protection for works on an ongoing basis. Therefore such systems should allow for the revocation of compromised or cloned devices. Furthermore the technologies embodied in these systems should be renewable so that a single hack does not destroy the efficacy of the system (*ibid.*).

<sup>212</sup> *Ibid.*

The development of and the implementation of protection technologies by commercial licensing agreements are only two parts of the copy-protection equation. Strong legal protection is also required.<sup>213</sup>

### **2.4.3 The Need for Statutory Regulation**

Technological protection measures and cross-industry agreements alone are not sufficient to protect authors' rights. Legal rules have to be formulated to ensure that protection technologies are respected and to deter the defeat of these measures by parties that might otherwise violate authors' rights.<sup>214</sup>

Not only authors, but also copyright users, telecommunications and equipment providers, and consumer electronics and computer manufacturers will benefit from the legal protection of technological protection measures. Authors will benefit because their economic and moral rights will be protected. Since technological protection measures deter piracy and encourage authors to use new media, new ways are opened for users to enjoy copyright works.

Telecommunications and equipment providers will benefit, as they profit from the increased traffic and legitimate electronic commerce in copyright material. And consumer electronics and computer manufacturers, who develop equipment and encryption technologies to play protected material, find their innovation frustrated and their investment rendered worthless if technological protection measures can be neutralized by hacking.<sup>215</sup>

Although it was common cause that statutory regulation and the protection of these new technologies were needed, several questions arose: Was the adoption of legislation shielding technological protection measures against 'circumvention' premature? Were existing rules adequate to address circumvention? If not, under what legal regime should technological protection measures be protected? And how should these legal rules be drafted?<sup>216</sup>

---

<sup>213</sup> Idem at 211-212.

<sup>214</sup> Idem at 200.

<sup>215</sup> <<http://www.ifpi.org/site-content/library/wipo%20treaties%20-%20technical%20measures.pdf>>, visited on 5 April 2002.

It was argued that the statutory regulation of technological protection measures was premature. It was yet uncertain how technology would develop, and specifically how it would affect authors' rights. Any regulation would be based on pure conjecture as to what might happen in future, and would be bound to be overtaken by technological and market developments. Less regulation was advocated; general clauses instead of fine-tuned, detailed regulation, since it was feared that further regulation might stifle the development of multimedia. It was better to rely on existing laws, and only where they proved to be inadequate, to address each specific problem as it arose.<sup>217</sup>

It was contended that the following existing legal principles adequately addressed the problem of protecting technological protection measures.<sup>218</sup> In the first instance, under the Berne Convention, authors had the right to sue primary infringers who use circumvention devices to facilitate infringing uses.<sup>219</sup> Secondly, under the laws of most, if not all, Berne Union members, authors had the right to sue those who facilitate infringement by others for contributory<sup>220</sup> or secondary infringement.<sup>221</sup> Thirdly, unfair competition law has been successfully used to attack circumvention devices.<sup>222</sup> Fourthly, the software industry thrived under article 7 of the Computer Programs Directive, which had been implemented in national laws. If article 7 did not provide adequate protection, the software industry, which had been

---

<sup>216</sup> Vinje op cit note 52 at 439.

<sup>217</sup> Ibid; Werner Rumphorst 'Fine-tuning Copyright for the Information Society' [1996] *European Intellectual Property Review* 79 at 81.

<sup>218</sup> See Séverine Dusollier 'Situating legal protections for copyright-related technological measures in the broader legal landscape: ANTI CIRCUMVENTION PROTECTION OUTSIDE COPYRIGHT' *General Report I.C. ALAI 2001 Congress, New York*, June 13-17 accessible at <[http://www.law.columbia.edu/conferences/2001/3\\_reports-en.htm](http://www.law.columbia.edu/conferences/2001/3_reports-en.htm)> (visited on 30 September 2002) for a general discussion of legal remedies for the circumvention of protection technologies outside the scope of law of copyright.

<sup>219</sup> Berne Convention for the Protection of Literary and Artistic Works (Paris Act 1971), articles 8, 9, 11, 11bis, 11ter, 12, 14 and 14bis and the South African Copyright Act of 1978, section 23(1) read together with sections 6-11B.

<sup>220</sup> See, for example, the South African Copyright Act, section 23(1) that provides that copyright is also infringed by any person who 'does or causes any other person to do' a restricted act without the authority of an author.

<sup>221</sup> See, for example the South African Copyright Act, section 23(2) and (3).

<sup>222</sup> It is interesting to note that Japan chose to reflect its commitment to implement and ratify the WCT by revising its Unfair Competition Prevention Law. On February 4, 1999, Japan's Ministry of International Trade and Industry announced a Bill to revise Japan's Unfair Competition Prevention Law which, inter alia, prohibits the production and sale of devices that circumvent or remove the copy protection functions on videos and compact discs. The Bill has been passed by the Japanese Diet on June 15, 1999 and came into effect on October 1, 1999. See John Tessenhojn 'A New Dawn in the Japanese Fight against Digital Piracy' (1999) 10 *Entertainment Law Review* 186 at 186-187.

subject to digital piracy for years, would not have thrived as it did.<sup>223</sup> Also, technological protection systems could be protected by combining them with contractual conditions.<sup>224</sup>

Several arguments were also raised that the protection of technological protection measures would infringe on the public's right to information. This argument is, however, unsubstantial. The right to information as such should be distinguished from the right to access to copyright works: free access to information does not imply free access to copyright works.<sup>225</sup>

However, despite these arguments, it was clear that present laws did **not** provide solutions to all the problems caused by digital development.<sup>226</sup>

‘The present confronts us with specific laws which exist and are enforceable. The great dilemma here is that virtually all these laws - to say nothing of the relevant conventions - were made before the digital era was even dreamt of. As a result, they need to be stretched and twisted, and to be interpreted in an open, progressive spirit. In some cases this may be possible, in others not.’<sup>227</sup>

Accordingly, lawyers and politicians were divided into two groups. The one group was of the opinion that although technological protection devices should be protected, they should not be protected by intellectual property laws. The second group argued that a ‘fine-tuned’ copyright law was the appropriate legal regime to regulate and protect new technology.

#### **2.4.3.1 Anti-Intellectual Property Response**

Especially members of the Internet community were frustrated by the way digital media was dealt with by the established copyright and patent regime and advocated an anti-intellectual property response.<sup>228</sup>

---

<sup>223</sup> Vinje op cit note 52 at 439.

<sup>224</sup> A problem with this solution is, however, that contracts are unenforceable against non-parties. Lucas op cit note 108 at 231.

<sup>225</sup> Idem at 234.

<sup>226</sup> Rumphorst op cit note 217 at 81.

<sup>227</sup> Idem at 80.

<sup>228</sup> See, for example, Johnson & Post op cit note 86 at 1367-1402.

According to Barlow,<sup>229</sup> intellectual property law

‘cannot be patched, retrofitted, or expanded to contain the gasses of digitised expression any more than real estate law might be revised to cover the allocation of broadcasting spectrum. . . . We will need to develop an entirely new set of methods as befits this entirely new set of circumstances.’

Digital technology differs from other technology, and it is appropriate to consider whether the copyright system should be adopted to accommodate the difference.<sup>230</sup> The rejection of regulation by copyright law is based on the following arguments.

In the first instance, traditional legal systems (such as copyright law) regulate physical, geographically defined territories, whereas cyberspace transcends territories and geographical borders.<sup>231</sup> Even within the 1989 WIPO Committee of Experts on a Possible Protocol to the Berne Convention doubts were raised as to whether copyright should be the applicable legal dispensation, because traditional copyright principles are based on national boundaries whereas national borders basically disappear in the digital world.<sup>232</sup>

Secondly, traditionally copyright protects the ‘expression’ of an idea, not the ‘idea’ itself (the so-called idea/expression dichotomy).<sup>233</sup> So copyright protection requires reduction to material form. Reduction to material form does not take place in a digital environment. Because of the dematerialization of works,<sup>234</sup> the supporting media of works are irrelevant or non-existent. Since ‘[i]t is now possible to convey ideas from one mind to another without ever making them physical, we are now claiming to own ideas themselves, not merely their expression’.<sup>235</sup> Copyright also depends on a distinction between the intellectual property right

---

<sup>229</sup> John Perry Barlow ‘Selling Wine Without Bottles. The Economy of Mind on the Global Net’ in P Bernt Hugenholtz (ed.) *The Future of Copyright in a Digital Environment* (1996) 169 at 170.

<sup>230</sup> Vinje op cit note 52 at 439.

<sup>231</sup> See, for example, Johnson & Post op cit note 86 at 1370-1371, 1383.

<sup>232</sup> Mort op cit note 89 at 189-190.

<sup>233</sup> Christie op cit note 6 at 528.

<sup>234</sup> Graham J H Smith ‘The Future of Intellectual Property in an Online World’ (1996) 7 *Computers and Law* 33.

<sup>235</sup> Barlow op cit note 229 at 173.

in a work and the right to the physical form in which the copyright finds expression.<sup>236</sup> In the digital world it is no longer possible to make this distinction - the copyright work and its mode of storage or delivery cannot be separated.<sup>237</sup>

Thirdly, a problem with the dematerialization of works is that the distinction between the different categories of works is blurred. Traditionally, copyright law protected certain categories of works, and in some instances the exclusive rights granted in relation to these categories differed. But it is difficult, if not impossible, to fit a multimedia work into only one of the traditional categories of works.<sup>238</sup>

Fourthly, a solution that would connect the fate of technological protection measures with copyright law would not be easy to implement. Such connection would require technological protection measures sufficiently rigid to deter hackers but flexible enough to allow uses in terms of the exceptions to and the limitations on an author's exclusive rights such as fair use, and so on.<sup>239</sup>

Fifthly, a copyright solution would imply that only technological protection measures shielding data protected by copyright would enjoy protection. Separate legislative measures would then be needed to protect technological protections shielding data not protected by copyright, such as news of the day and works in the public domain.

The approach of prohibiting in principle the circumvention of security devices, regardless of whether the works of authorship are the object of exclusive rights, is simpler and more efficient. Accordingly, it could be more appropriate to distinguish the remedies for copyright infringement from those aimed at circumvention as such, while maintaining that they may apply concurrently.<sup>240</sup>

#### **2.4.3.2 Intellectual Property Response**

---

<sup>236</sup> *Idem* at 170.

<sup>237</sup> Fitzpatrick op cit note 103 at 217.

<sup>238</sup> Christie op cit note 6 at 525.

<sup>239</sup> Lucas op cit note 108 at 237.

This school of thought reflects the majority opinion<sup>241</sup> and argues that the existing copyright law needs only ‘fine-tuning’ in order to deal with the demands of the digital age.<sup>242</sup>

Intellectual property is seen as the only realistic legislative solution for new technology.

They advance the following arguments for regulating new technology by law of copyright:

In the first instance, although the Internet is a new medium for transmitting information, the content remains words, sounds, and images - they just happen to be conveyed in binary form.<sup>243</sup> So the content can, just like in the analogue world, constitute works protected by copyright and works not protected by copyright.

Secondly, with regards to the dematerialization of works, copyright law does not fundamentally protect a tangible form of expression but rather the author’s intellectual creation expressed in such form. Although digitization changed the format in which works are expressed, the substance of an author’s intellectual creations has not changed. Copyright law protects an author’s intellectual creation, over and above the tangible form of such expression, the physical media on which such creation is recorded, or the mechanical means by which such expression is delivered.<sup>244</sup> The fundamentals of copyright remain the same regardless of the format in which the works are expressed. So the digital format of works does not radically undermine the bases of copyright laws conceived in an analogue world.<sup>245</sup>

Thirdly, the fundamental copyright principle that there is a property right – copyright - in every work that first belongs to the author of that work has not changed. Only the nature of the author’s property right has changed with technology, and will change even further.<sup>246</sup>

Fourthly, the advantage of a correlation with copyright law is that it legitimizes legislative

---

<sup>240</sup> Ibid.

<sup>241</sup> It is the approach retained by the United States proposal. The European Commission and Member States have adopted a similar position in the course of negotiations on the Berne Convention Protocol. Lucas op cit note 108 at 235.

<sup>242</sup> See, for example, Johnson & Post op cit note 86 at 1367-1402; Rumphorst op cit note 217 at 81; Dixon & Self op cit note 26 at 465-472 and Lucas op cit note 108 at 226.

<sup>243</sup> Fitzpatrick op cit note 103 at 218.

<sup>244</sup> Dixon & Self op cit note 26 at 468.

<sup>245</sup> Fitzpatrick op cit note 103 at 218.

intervention. This is especially important where the implementation of criminal sanctions is considered. Criminal law should not interfere with private interests, even if the development of global information networks actually interests all of us collectively. Copyright law and neighbouring rights are an excellent pretext to reintroduce public policy considerations, since the law already provides for criminal sanctions in that context.<sup>247</sup>

At this point it is important to note that only technological protection measures shielding data protected by copyright should be protected by copyright law. There is no reason to extend copyright protection to data simply because it is protected by technological protection measures. Technological protection measures applied to other categories of data should not be protected by copyright law but by separate dedicated legislation.

So the remedies should be available only if the circumvention of the security devices triggers an infringement of copyright law or neighbouring rights.<sup>248</sup>

Even though technology and social change have brought other activities within the ambit of copyright scrutiny and changed the method of expression of original creative ideas, copyright law remains the only solution.

Bowrey<sup>249</sup> states that

‘[c]opyright . . . is not merely an historical artefact of the Second Wave, with inflexible legal categories. Copyright is a complex organic body of law, containing possibilities for development, re-development and reform.’

## **2.5 Conclusion: The WIPO Copyright Treaty**

As I shall show below, the international community saw the need for the statutory regulation of technological protection measures. Despite the voices raised in favour of sui generis

---

<sup>246</sup> Barrow op cit note 111.

<sup>247</sup> Lucas op cit note 108 at 237.

<sup>248</sup> Idem at 235.

<sup>249</sup> Kathy Bowrey ‘Who’s Writing Copyright’s History?’ [1996] *European Intellectual Property Review* 322-

regulation, it was decided that legislation relating to technological protection measures should be added to the armoury of intellectual property laws. Consequently, an international treaty, the WIPO Copyright Treaty, was drafted and adopted to deal, on the basis of copyright principles, with the technological challenges.<sup>250</sup>

---

329 at 328; Dixon and Self *op cit* note 26 at 468.

<sup>250</sup> Although the WCT is not a protocol to the Berne Convention, its 'objective is ... to supplement and update the international regime ... based fundamentally on the Berne Convention.' Since the WCT is based on the Berne Convention, and the Berne Convention regulates copyright, it is clear that the WCT is based on copyright principles. It makes it clear that copyright applies on the Internet as it does in the off-line world. It supplements the Berne Convention by providing copyright protection while considering the need for the free flow of information (Mort *op cit* note 88 at 196).

## CHAPTER 3: THE CREATION OF NEW INTERNATIONAL NORMS – THE WIPO COPYRIGHT TREATY

‘The time has come’, the Walrus said,  
    ‘To talk of many things:  
Of shoes - and ships - and sealing wax -  
    Of cabbages - and kings -  
And why the sea is boiling hot -  
    And whether pigs have wings.’

LEWIS CARROL

*Through the Looking-Glass and What Alice Found There*

### 3.1 Background

Since the late nineteenth century, international conventions have governed the protection of intellectual property. These conventions provide the minimum standard of protection guaranteed by the international community.<sup>1</sup>

The Berne Convention for the Protection of Literary and Artistic Works was adopted in 1886. It was the first and most important treaty in the field of copyright and was revised quite regularly in order to provide solutions to problems caused by developments such as phonography, photography, radio, cinematography, and television.<sup>2</sup>

In the field of neighbouring (or related) rights, the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (the Rome Convention) was adopted in 1961.<sup>3</sup> It has not been revised since its adoption.<sup>4</sup> Two new

---

<sup>1</sup> Susan A. Mort ‘The WTO, WIPO & the Internet: Confounding the Borders of Copyright and Neighboring Rights’ (1997) 8 *Fordham Intellectual Property, Media and Entertainment Law Journal* 173 at 178.

<sup>2</sup> Dr Mihály Fiscor ‘The Spring 1997 Horace S. Manges Lecture - Copyright for the Digital Era: The WIPO “Internet” Treaties’ (1997) 21 *Columbia - VLA Journal of Law and the Arts* 197 at 197.

<sup>3</sup> Wend Wendland ‘The Digital Agenda’ (1997) 5 *JBL* 143.

<sup>4</sup> Reinbothe and Lewinski offers as possible reasons the fact that it was administered jointly by WIPO, the International Labour Organisation and UNESCO; and, that besides the resulting organisational problems, the coverage of three groups of rightholders with partly diverging interests might have been perceived by some as difficult (see Jörg Reinbothe & Silke von Lewinski ‘The WIPO Treaties 1996: Ready to Come into Force’

conventions have been adopted since then in the field of neighbouring rights: the Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of Their Phonograms in Geneva in 1971, and the Convention Relating to the Distribution of Programme-Carrying Signals Transmitted by Satellite.<sup>5</sup>

Numerous technological and commercial developments took place since the adoption of these conventions and the last revision of the Berne Convention in Paris in 1971. These developments made further international regulation necessary.

Rather than revising the treaties themselves to regulate these developments, the international community adopted a strategy of ‘guided development’. ‘Guided development’ involved the making of recommendations, guiding principles, and model provisions worked out by the various World Intellectual Property Organization (WIPO)<sup>6</sup> bodies. These recommendations and principles were mainly based on the interpretation of existing international norms, but they also included some new standards.<sup>7</sup>

At the end of the 1980s it was, however, recognized that mere guidance was not sufficient any longer and that new international norms were needed.<sup>8</sup> Because of the global character of these developments, mere national regulation would have been insufficient – the adoption of new international instruments was needed.<sup>9</sup> So the time came to start negotiating provisions for the adoption of international instruments to regulate these new developments.

The preparation of the new legal norms started in the General Agreement on Trade and Tariffs (GATT) and in WIPO. The preparations in GATT lead to the adoption of the

---

[2002] *European Intellectual Property Review* 199 at 200).

<sup>5</sup> Mihály Ficsor *The Law of Copyright and the Internet: The 1996 WIPO Treaties, their interpretation and Implementation* (2002) at 4.

<sup>6</sup> The World Intellectual Property Organization (WIPO) is a specialized agency of the United Nations that has responsibility for, among other things, hosting discussions and negotiations concerning international intellectual property norms (Pamela Samuelson ‘The U.S. Digital Agenda at WIPO’ (1997) 37 *Virginia Journal of International Law* 369 at 369 note 1).

<sup>7</sup> Ficsor op cit note 2 at 197-198.

<sup>8</sup> Idem at 198.

<sup>9</sup> Mort op cit note 1 at 175; Thomas C Vinje ‘A Brave new World of Technical Protection Systems: Will There Still Be Room For Copyright?’ [1996] *European Intellectual Property Review* 431 at 439; Simon Fitzpatrick ‘Copyright Imbalance: U.S. and Australian Responses to the WIPO Digital Copyright Treaty’ [2000] *European*

Agreement on Trade-Related Aspects of Intellectual Property Rights (the TRIPS Agreement).<sup>10</sup> The purpose of the TRIPS Agreement is to provide minimum standards with which countries' intellectual property laws must comply, and for the proper and adequate means to enforce those rights.<sup>11</sup> It included certain results of the period of 'guided development'. However, even though the TRIPS Agreement applies to many of the issues raised by digital technology, it does not contain any provisions concerning technological protection measures, or rights management information.<sup>12</sup>

The issue of technological protection measures and rights management information was addressed only towards the end of the 'guided development' period, in the (unfinished) preparatory work of the WIPO Model Provisions for Legislation in the Field of Copyright and the WIPO Model Law on the Protection of Producers of Phonograms. The documents prepared for the Committees of Experts dealing with the Model Provisions and Model Law, respectively, and the discussions at the sessions of those committees provided useful material on these issues for the later preparatory work of the WCT and WPPT.<sup>13</sup>

In 1989, WIPO organized the Committee of Experts on a Possible Protocol to the Berne Convention 'destined to clarify the existing, or establishing new, international norms where, under the present text of the Berne Convention, doubts may exist as to the extent to which that Convention applies'.<sup>14</sup> A few years later, WIPO convened, in parallel, a Committee of Experts on a Possible Instrument for the Protection of the Rights of Performers and Producers of Phonograms. These Committees had met, respectively, in seven and six sessions until May 1996.<sup>15</sup> The working papers prepared for the first two sessions of the Berne Protocol Committee did not include any proposals concerning technological protection measures, or rights management information.<sup>16</sup> Before its third session, the issues of reference of the

---

*Intellectual Property Review* 214 at 217.

<sup>10</sup> Ibid.

<sup>11</sup> Part III section 1 Article 41, Section 2 Article 42-49.

<sup>12</sup> Ficsor op cit note 2 at 198. Ficsor op cit note 5 para 6.01 at 359.

<sup>13</sup> Ficsor op cit note 5 at 359-360.

<sup>14</sup> Basic Proposal on the Substantive Provisions of the Treaty on Certain Questions Concerning the Protection of Literary and Artistic Works to be Considered by the Diplomatic Conference, at ¶ 1, WIPO CRNR/DC/4 (30 August 1996), accessible at <[http://www.uspto.gov/web/offices/dcom/olia/diplconf/4dc\\_a13.htm](http://www.uspto.gov/web/offices/dcom/olia/diplconf/4dc_a13.htm)> (visited on 27 June 2002).

<sup>15</sup> Reinbothe & Lewinski op cit note 4 at 200.

<sup>16</sup> Ficsor op cit note 5 para 6.39 at 384.

Committee were modified. The enforcement of rights was one of the ten issues to be covered. The working paper for the third session interpreted the ‘enforcement of rights’ extensively also to cover ‘measures concerning abuses in respect of technical devices’.<sup>17</sup>

The proposed draft provisions were based on the ideas discussed in the ‘guided development’ period. They followed the same approach and covered two different cases: protection against the circumvention of anti-copying devices, and protection against illegal decoders.<sup>18</sup>

The issues relating to digital technology were only discussed as of 1994/1995.<sup>19</sup>

A Diplomatic Conference on Certain Copyright and Neighbouring Rights Questions was convened in Geneva from 2 to 20 December 1996. Three proposals were discussed. The first proposal, relating to the ‘Treaty on Certain Questions Concerning the Protection of Literary and Artistic Works’, was to expand the rights provided for under the Berne Convention; the second proposal, relating to the ‘Treaty for the Protection of the Rights of Performers and Producers of Phonograms’, was to provide new rights for performers and the producers of phonograms (sound recordings); and the third proposal, relating to the ‘Treaty on Intellectual Property in Respect of Databases’, was to provide sui generis protection for compilations of data.<sup>20</sup>

In the end, the Diplomatic Conference reached agreement on the first two proposals. Two treaties, the WIPO Copyright Treaty (the WCT) and the WIPO Phonograms and Performances Treaty (the WPPT), were adopted. These two treaties contain broad provisions that apply to a variety of situations involving information technologies. They are important both for their intellectual property principles and their effect upon international trade.<sup>21</sup>

---

<sup>17</sup> Idem para 6.40 at 384-385.

<sup>18</sup> Ibid.

<sup>19</sup> Reinbothe & Lewinski op cit note 4 at 200.

<sup>20</sup> Heather Rosenblatt ‘Protocol to the Berne Convention The WIPO Diplomatic Conference - the Birth of Two New Treaties’ (1997) 13 *The Computer Law & Security Report* 307; David Nimmer ‘A Tale of Two Treaties: dateline Geneva - December 1996’ (1997) 22 *Columbia - VLA Journal of Law and the Arts* 1 at 4; and Mort op cit note 1 at 191.

<sup>21</sup> Mort op cit note 1 at 175, 176 and 194.

The database proposal was not considered and was deferred for later discussion.<sup>22</sup>

The WCT entered into force on 6 March 2002,<sup>23</sup> and the WPPT on 20 May 2002.<sup>24</sup>

The WCT thus developed in the same way as the previous five revisions and the two additions to the Berne Convention did – not as a radical change to authors’ rights but as an evolution and refinement of those rights. It confirms consensus views, addresses new technology, and responds to legal and political developments that have arisen since the previous revisions to the Convention.<sup>25</sup> However, unlike the previous revisions, the WCT was not a reaction to developments in technology and the market. Rather, it prepared the ground for the functioning of the new services of the information society with due regard to intellectual property. In this sense, the WCT and the WPPT are unusual international instruments given the history of international law making – such law making is usually reactive rather than proactive.<sup>26</sup>

### **3.2 Interpreting the WCT**

At its inception the WCT was planned as a protocol to the Berne Convention. The instrument that emerged from the Diplomatic Conference, is however, not accessory to the Berne Convention. It rather supplements and updates the international regime based fundamentally on the Berne Convention.

The nature of the WCT appears from article 1.1 which states that ‘[t]his Treaty is a special agreement within the meaning of Article 20 of the Berne Convention for the Protection of Literary and Artistic Works, as regards Contracting Parties that are countries of the Union established by that Convention’.

Article 20 of the Berne Convention states that ‘[t]he governments of the countries of the

---

<sup>22</sup> See Nimmer op cit note 20 at 1-4; and Mort op cit note 1 at 195.

<sup>23</sup> <<http://www.wipo.int/pressroom/en/releases/2002/p304.htm>> (visited on 14 March 2002).

<sup>24</sup> Ibid.

<sup>25</sup> Allen N Dixon & Martin F Hansen ‘The Berne Convention Enters the Digital Age’ [1996] *European Intellectual Property Review* 604.

Union reserve the right to enter into special agreements among themselves, in so far as such agreements grant to authors more extensive rights than those granted under the Convention. . . . As the WCT, then, is a special agreement under article 20 of the Berne Convention, it has to raise the level of protection previously granted under the Berne Convention.<sup>27</sup> The WCT accordingly reflects the desire to supplement international copyright protection in new areas, without detracting from the existing rights under the Berne Convention.<sup>28</sup> As a special agreement under this Convention, the WCT did not, unlike a revision of the Convention, require unanimity of the negotiating parties.<sup>29</sup>

The WCT, like the TRIPS Agreement, obliges Contracting Parties to comply with articles 1 to 21 of the Berne Convention and the appendix to it. Unlike the TRIPS Agreement, the WCT does not exclude article 6bis of the Berne Convention (on moral rights) from this obligation.<sup>30</sup>

Article 1.1 of the WCT is thus of special importance to the interpretation of this treaty. No interpretation of the WCT can be sustained that may result in a decrease of the level of the protection of authors under the Berne Convention.<sup>31</sup> By granting more extensive rights to authors, the rights of copyright users are correspondingly diminished.

The WCT extends the existing rights under the Berne Convention in two ways: directly by establishing three crucial rights of authors – distribution,<sup>32</sup> rental,<sup>33</sup> and communication to the public,<sup>34</sup> and indirectly by creating two additional types of infringement – the circumvention

---

<sup>26</sup> Reinbothe & Lewinski op cit note 4 at 199.

<sup>27</sup> Nimmer op cit note 20 at 10.

<sup>28</sup> Mort op cit note 1 at 197-198.

<sup>29</sup> Reinbothe & Lewinski op cit note 4 at 200.

<sup>30</sup> Ibid.

<sup>31</sup> Fiscor op cit note 2 at 199-200.

<sup>32</sup> Article 6 of the WCT. Authors of literary and artistic works have not been granted a general right of distribution under any existing international agreement. The Berne Convention contains a right of distribution only in respect of cinematographic works. Article 6 of the WCT extends the right of distribution to all categories of works.

<sup>33</sup> Article 7 of the WCT. The Berne Convention does not contain any provisions on the rental of copies of literary and artistic works. Article 7 of the WCT creates a new right of rental in respect of computer programs, cinematographic works and works embodied in phonograms.

<sup>34</sup> Article 8 of the WCT. In the Berne Convention the exclusive right of communication to the public has been regulated in a fragmented manner by articles 11, 11bis, 11ter, 14 and 14bis. The right of communication to the public has now been clarified and the field of application extended to cover all categories of works by article 8

of technological protection measures,<sup>35</sup> and the removal or alteration of rights management information.<sup>36</sup>

### 3.3 Technological Protection Measures

During the preparatory work in WIPO it was recognized that it was not sufficient merely to provide for appropriate rights in respect of the digital uses of works. No rights can be applied effectively in the digital world without the support of technological measures necessary to licence and monitor uses. But there was a constant concern that technology will be developed and marketed to circumvent or alter these technological systems of protection.<sup>37</sup> Although the application of protection measures should be left to the interested authors, appropriate legal protection for these measures was needed.<sup>38</sup>

Articles 11 and 12 of the WCT create two new types of indirect copyright infringement to provide legal protection for technological protection measures. Whereas other provisions of the WCT effectively interpret and adapt existing international copyright norms, articles 11 and 12 create new norms.<sup>39</sup> The WCT precedes any such provisions in national law. It goes without saying that the obligation to provide adequate sanctions against the circumvention of technological protection measures and the removal or alteration of rights management information considerably strengthens the functioning of author's rights in the digital environment.<sup>40</sup>

In this I shall limit my discussion to article 11 of the WCT.

The Chairman of the Committee of Experts on the Protocol to the Berne Convention prepared a Basic Proposal (the Basic Proposal for the Substantive Provisions of the Treaty<sup>41</sup>) which

---

of the WCT.

<sup>35</sup> Article 11 of the WCT.

<sup>36</sup> Article 12 of the WCT.

<sup>37</sup> Vinje op cit note 9 at 431.

<sup>38</sup> Ficsor op cit note 2 at 216.

<sup>39</sup> Ficsor op cit note 5 at 544.

<sup>40</sup> Reinbothe & Lewinski op cit note 4 at 201.

<sup>41</sup> Basic Proposal op cit note 14.

formed the basis of the negotiations in Geneva.<sup>42</sup>

In order to understand article 11 of the WCT, it is important to see how the Contracting Parties came to decide on its wording. So I shall discuss the provisions of the Basic Proposal and then also examine the United States and European proposals before I discuss the final text of the treaty.

### **3.3.1 The Proposals for the Prohibition on Circumvention Devices**

#### **3.3.1.1 The United States Proposal**

The Clinton Administration proposed the following wording for inclusion in a protocol to the Berne Convention:

‘Contracting Parties shall make it unlawful to import, manufacture or distribute any device, product, or component incorporated into a device or product, or offer or perform any service, the primary purpose or effect of which is to avoid, bypass, remove, deactivate, or otherwise circumvent, without authority, any process, treatment, mechanism or system which prevents or inhibits the unauthorised exercise of any of the rights under the Berne Convention or this Protocol.’<sup>43</sup>

During the run-up to the 1996 Diplomatic Conference the United States submitted the most detailed proposal and comments.<sup>44</sup> The language in this proposal was nearly identical to the Clinton Administration’s.<sup>45</sup>

The White Paper motivated this broad prohibition of anti-circumvention devices by arguing that such an approach was not unprecedented. In support of this argument the White Paper

---

<sup>42</sup> Thomas C Vinje ‘All’s Not Quiet on the Berne Front’ [1996] *European Intellectual Property Review* 585.

<sup>43</sup> Proposals Submitted by the United States of America to the Committee of Experts on a Possible Protocol to the Berne Convention, Sixth Session, Geneva, 1 to 9 February 1996 (the ‘US proposal’).

<sup>44</sup> Ficsor op cit note 5 at 391.

<sup>45</sup> National Information Infrastructure Task Force, Report of the Working Group on Intellectual Property and the National Information Infrastructure (September 1995 (‘US White Paper’); HR 2441, 10th Cong., 1st Sess (1995); S 1284, 104th Cong., 1st Sess (1995) (hereafter jointly referred to as the ‘US White Paper Bill’).

referred to (a) the Audio Home Recording Act<sup>46</sup> (which regulates digital audio tape recorders); (b) section 605 of the Communications Act<sup>47</sup> (which regulates devices that can be used to decrypt satellite transmissions of television programmes); (c) a provision in the North American Free Trade Agreement (NAFTA) regarding decryption of satellite transmissions;<sup>48</sup> and (d) section 296(2) of the Copyright, Designs and Patents Act 1988 in the United Kingdom.<sup>49</sup>

Vinje<sup>50</sup> is of the opinion that the United States proposal was far broader than any of these precedents for the reasons that I set out below.

In the first instance, the precedents to which the White Paper referred were directed towards very specific, demonstrable problems and to very limited technologies. The United States proposal, by contrast, would apply to any device, product, or service, the primary purpose or effect of which is to circumvent any process, treatment, mechanism, or system that prevents or inhibits copyright infringement.<sup>51</sup> The actual language of the proposal extended broadly, far beyond technological protection devices. There was virtually no limit to the type of ‘protection device’ to which the proposal might extend, and hence an equally wide range of the type of ‘circumvention devices’ to which the proposal might apply.

Secondly, the unauthorized decryption of satellite cable broadcasts invariably involves gaining access to a signal to which the recipient has no legal entitlement. By contrast, technological protection systems shielded by the United States proposal had nothing to do with preventing access but only with controlling what could be done with works already in a user’s legitimate possession. So technological protection measures could prevent legitimate

---

<sup>46</sup> 17 USC § 1002(C).

<sup>47</sup> 47 USC § 605.

<sup>48</sup> NAFTA, art 1707(a).

<sup>49</sup> This provision states that ‘The person issuing the copies to the public has the same rights against a person who, knowing or having reason to believe that it will be used to make infringing copies—

‘(a) makes, imports, sells or lets for hire, offers or exposes for sale or hire, or advertises for sale or hire, any device or means specifically designed or adapted to circumvent the form of copy-protection employed, or

‘(b) publishes information intended to enable or assist persons to circumvent that form of copy-protection, as a copyright owner has in respect of an infringement of copyright.’

<sup>50</sup> Vinje op cit note 9 at 432.

<sup>51</sup> Ibid.

dealings by those in lawful possession of the copyright works.<sup>52</sup> The proposal thus had the potential of altering the existing copyright balance.<sup>53</sup>

Thirdly, the Audio Home Recording Act accommodated user interests and expectations in a way the United States proposal did not – the proposal did not accommodate fair use or user interests, because they shielded technological protection measures that did not permit any copy of a work, lawful or unlawful, to be made.<sup>54</sup>

Fourthly, although the United Kingdom statute is not limited to specific technologies, it does contain limitations. For one, it contains a knowledge requirement – it applies only to those who make devices ‘knowing or having reason to believe’ that they will be used to make infringing copies. Also, the statute applies only to devices or means ‘specifically designed or adapted’ to circumvent a copy protection system. Neither limitation is found in the United States proposal, although a knowledge requirement is included in the European proposal.<sup>55</sup>

The vagueness of the United States proposal is exacerbated by the uncertainty surrounding the meaning of the phrase ‘primary purpose or effect’. Vinje argues that problem could be addressed by eliminating the ‘primary effect’ language but to clarify that the relevant purpose is that of the offending device manufacturer rather than the unpredictable purpose of the device’s end users. Devices obviously do not themselves have ‘purposes’, so the proposal must be taken to refer to the primary purpose of either the device manufacturer or the user – but it is difficult to determine whose.<sup>56</sup>

Vinje<sup>57</sup> believes that neither the United States nor the European proposal provided the degree of clarity and fairness that should be required of any such prohibition. In particular, under the United States proposal, a manufacturer would have virtually no way of knowing before producing and selling a device whether it would violate the provision. The proposal would impose liability on a manufacturer for the often unpredictable behaviour of other people – the

---

<sup>52</sup> *Idem* at 433.

<sup>53</sup> *Ibid.*

<sup>54</sup> *Idem* at 433-434.

<sup>55</sup> *Idem* at 434.

<sup>56</sup> *Idem* at 435.

consumer users of the device. Specifically, by prohibiting devices based on their primary purpose or effect, the proposal places a manufacturer in a position where he could be forced to take a device off the market because of the unpredictable activities of the purchasers of the device. This could lead to a situation where manufacturers would avoid the development of legitimate new technologies, to the detriment of consumer welfare.<sup>58</sup>

The ‘without authority’ language appears to apply either to the importation, manufacture, or distribution of an offending device, or to the act of disabling or circumventing the anti-copy technology. However, neither the fair use doctrine nor any other provision of copyright right law will ‘authorize’ the manufacture of a device or the circumvention of anti-copy technology. Rather, copyright law ‘authorizes’, in some circumstances, the reproduction that an anti-copy technology can prevent and a circumvention device can facilitate. In short, then, the ‘without authority’ language is simply misplaced.<sup>59</sup>

Although the White Paper claims that even if its proposal does shield the technological protection of works in the public domain, such protection would extend ‘only to those particular copies – not to the underlying works itself’.<sup>60</sup> It is not clear on which basis the authors of the White Paper would require a user with lawful access to a work to take the time and incur the expense of obtaining alternative access to that work in order to make a copy of the work that he is legally entitled to make. Would this create incentives for firms to buy up the public domain and put it online, subject to technological protection?<sup>61</sup>

Where a work is protected by a technological protection measure, the provisions of the White Paper could also have dire consequences for those who need to reverse engineer the protected work in order to obtain interoperability.

The term ‘interoperability’ connotes the ability of software and hardware manufactured by different developers to be used together. To achieve interoperability, software and hardware

---

<sup>57</sup> Idem at 434.

<sup>58</sup> Ibid.

<sup>59</sup> Idem at 437.

<sup>60</sup> US White Paper Bill op cit note 45.

<sup>61</sup> Vinje op cit note 9 at 437.

developers must have access to the interface specifications of their competitors. When this information is not available, reverse engineering may be required to discover it.<sup>62</sup> This reverse engineering process technically requires ‘reproductions’ and ‘translations’ to be made of the software being analysed. To ensure the ability to achieve interoperability, copyright law, generally, permits the reproduction and translation activities inherent in software reverse engineering.<sup>63</sup>

The problem arising in this context is the following: developers can include technological means in their software that prevent not only unlawful copying but that also the lawful copying inherent in software reverse engineering. Another developer may then create a device for circumventing the reverse engineering ‘lock’ to facilitate lawful recompilation for interoperability purposes. However, that device may also be capable of being used to circumvent the protection system for purposes of unlawful reproduction. Although a device that circumvents a reverse engineering ‘lock’ clearly would have a lawful use, like many such devices it could also have unlawful uses. And even though the device’s developer would intend for it to be used lawfully, he would have no way of knowing in advance whether it would actually be used primarily for lawful or unlawful purposes.<sup>64</sup>

A developer seeking to eliminate legitimate competition by preventing reverse engineering may then claim that the circumvention device (or perhaps even the reverse engineering itself) has the ‘primary purpose or effect’ of circumventing a mechanism ‘which prevents or inhibits the infringement’ of its rights. Accordingly, unless properly limited, a treaty provision may allow companies to prevent, through technological means, reverse engineering that they could not prevent through copyright.<sup>65</sup>

### **3.3.1.2 The European Commission Proposal**

Most of the objections to the United States proposal can also be raised to the European

---

<sup>62</sup> Ibid.

<sup>63</sup> Idem at 438; Thomas Vinje ‘Copyright Imperilled?’ [1999] EIPR 192 at 193. The exceptions for reverse engineering are also contained in Article 6, Council Directive 91/250/EEC of 14 May 1991 on the Legal Protection of Computer Programs, OJ L 122, 17/05/1991 P. 0042 - 0046 (‘Computer Programs Directive’).

<sup>64</sup> Vinje op cit note 9 at 438.

Commission proposal.

Like its American counterpart, the European proposal is not limited to specific technologies,<sup>66</sup> and there is no limitation on the type of ‘protection device’ to which it might extend.

It would also prevent legitimate possessors of copyright works from doing what the law permits them to do, and so can alter the existing copyright balance in favour of authors.<sup>67</sup> In particular, it does not provide for fair use or users’ interests.<sup>68</sup>

However, unlike the United States proposal, the European proposal does include a knowledge requirement.<sup>69</sup>

As I have indicated, the meaning of the phrase ‘primary purpose or effect’ is uncertain. Both the American and European proposals refer to the purpose of the circumvention device, which should be read to refer to the primary purpose of either the device manufacturer or the user.<sup>70</sup> As I have shown, this could lead to a situation where manufacturers would avoid the development of legitimate new technologies, which would be to the detriment of the consumer.<sup>71</sup>

The ‘without authority’ language in the European proposal was as objectionable as that in the United States proposal.<sup>72</sup>

Finally, fair use and interoperability would have been endangered had the language been adopted as it stood.

### **3.3.1.3 The African Proposal**

---

<sup>65</sup> Ibid.

<sup>66</sup> Idem at 432.

<sup>67</sup> Idem at 433.

<sup>68</sup> Idem at 433-434.

<sup>69</sup> Idem at 434.

<sup>70</sup> Idem at 435.

<sup>71</sup> Idem at 434.

At the 1996 Diplomatic Conference, South Africa, speaking for a group of African countries, proposed the current wording of article 11 of the WCT.<sup>73</sup> Its focus on acts of circumvention is a departure from its draft version which extended to devices.<sup>74</sup>

### **3.3.1.4 Article 13 of Basic Proposal for the Substantive Provisions of the Treaty<sup>75</sup>**

The legal protection of technological protection measures can be provided in two ways: by proscribing the devices used to circumvent these technologies, or by prohibiting the act of circumvention itself.<sup>76</sup>

Article 13 of the Basic Proposal<sup>77</sup> reads as follows:

‘Obligations concerning Technological Measures

‘(1) Contracting Parties shall make unlawful the importation, manufacture or distribution of protection-defeating devices, or the offer or performance of any service having the same effect, by any person knowing or having reasonable grounds to know that the device or service will be used for, or in the course of, the exercise of rights provided under this Treaty that is not authorized by the rightholder or the law.

‘(2) Contracting Parties shall provide for appropriate and effective remedies against the unlawful acts referred to in paragraph (1).

‘(3) As used in this Article, “protection-defeating device” means any device, product or component incorporated into a device or product, the primary purpose or primary effect of which is to circumvent any process, treatment, mechanism or system that

---

<sup>72</sup> *Idem* at 437.

<sup>73</sup> Amendments to articles 7, 10, 13 and 14 of Draft Treaty N° 1 proposed by the Delegations of Algeria, Angola, Burkina Faso, Cameroon, Chad, Côte d’Ivoire, Egypt, Ethiopia, Gabon, Gambia, Ghana, Kenya, Lesotho, Libya, Madagascar, Malawi, Mali, Mauritius, Morocco, Namibia, Niger, Nigeria, Senegal, South Africa, Sudan, Togo, Tunisia, United Republic of Tanzania, Zambia and Zimbabwe, WIPO Document CRNR/DC/56 (12 December 1996) (the ‘African Proposal’).

<sup>74</sup> Vanessa van Copenhagen ‘Copyright and the WIPO Copyright Treaty, With Specific Reference to the Rights Applicable in a Digital Environment and the Protection of Technological Measures’ (2002) 119 *South African Law Journal* 429 at 442.

<sup>75</sup> Basic Proposal *op cit* note 14.

<sup>76</sup> Gregory C Ludlow ‘Copyright and the Challenge of the Digital World’ (1999) 3 *Canadian International Lawyer* 199 at 202.

prevents or inhibits any of the acts covered by the rights under this Treaty.’

These provisions are intended to ensure that the author’s exclusive rights to control the reproduction and distribution of her work are honoured.<sup>78</sup>

Paragraph (1) of the proposed article 13 prohibits five acts: the importation, manufacture, or distribution of protection-defeating devices, and the offer or performance or services that have the same effect.<sup>79</sup> The first three acts concern devices, and the last two the act of circumvention itself. Article 13 thus proposed to prohibit both devices used to circumvent technological protection measures as well as the act of circumvention itself.

There were many objections to the prohibition on protection defeating devices.

The first objection concerned the status of the Basic Proposal as a protocol to the Berne Convention. The Berne Convention does not, and never has, prohibited any particular device by means of which infringement occurs. Instead, it has always regulated the acts that constitute infringement.<sup>80</sup>

A second objection was that the fact that a work that is not protected by copyright does not preclude an online content owner or service provider from shielding it behind technological protection measures. A user cannot compel such a content owner or service provider to guarantee unrestricted access to and use of a work simply because it is in the public domain. Similarly, the fact that a work is subject to a number of exceptions<sup>81</sup> does not mean that the author is obliged to help a user, who is authorized by a certain exception, to gain access to a work or to use it.<sup>82</sup> This means that works that are subject to exceptions and so can be used

---

<sup>77</sup> Basic Proposal op cit note 14.

<sup>78</sup> Dixon & Hansen op cit note 25 at 611.

<sup>79</sup> Note 13.02.

<sup>80</sup> Vinje op cit note 9 at 434.

<sup>81</sup> It is beyond the scope of this chapter to discuss whether users have a ‘right’ to demand access to and the making of non-infringing use of a copyright work. So in this chapter I have used the words ‘exception’ and ‘limitation’ to connote what is otherwise also referred to as ‘exemptions’ to the exclusive rights held by authors. I shall address this issue in Chapter 7.

<sup>82</sup> André Lucas ‘Copyright Law and Technical Protection Devices’ (1997) 21 *Columbia - VLA Journal of Law and the Arts* 225 at 236.

under copyright law may be ‘locked up’ by online content owners.<sup>83</sup> Accordingly, the argument continues, by including a prohibition on technological protection circumvention devices the proposed protocol runs the risk of undermining the copyright system, and effectively of replacing it with a system controlled by those using technological protection devices.<sup>84</sup> Moreover, even when these measures are used in relation to works protected by copyright, the author could in practice extend the term of protection indefinitely – the technological protection would prevent reproduction even after the copyright term has expired.<sup>85</sup>

A third objection is that the proposed prohibition of devices would undermine the existing balance of the rights achieved in the Berne Convention. It could upset the balance between the rights of authors and users by limiting exceptions or by closing access to works in the public domain.<sup>86</sup> It is not easy to draft a law on technical protection measures that maintains the existing balance. The proposal is not alike to a simple no-trespass law. Instead, it throws into doubt the continued viability of existing limits on rights and threatens to impoverish society by shrinking the public domain.<sup>87</sup> The proposal threatens to prevent not only copying that is bad but also copying that is of vital importance to society at large.<sup>88</sup> It could also upset the existing balance by subjecting innocent equipment manufacturers and distributors to liability if their devices were used by others to circumvent copy-protection measures.<sup>89</sup> Consumer electronics manufacturers argued that the proposed article 13 could be interpreted to require them to alter their equipment. By focussing on devices that could be used to circumvent technological protection measures rather than on the act of infringement, a significant risk arises that consumer electronics, general-purpose computers, and related hardware and software could be caught by the prohibition.<sup>90</sup>

---

<sup>83</sup> William Cornish & David Llewellyn *Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights* 5 ed (2003) at 796 and 808-12.

<sup>84</sup> Vinje op cit note 9 at 434.

<sup>85</sup> Jonathan Band, Taro Isshiki ‘The New US Anti-Circumvention Provision: Heading in the Wrong Direction’ (1999) 15 *Computer Law & Security Report* 220.

<sup>86</sup> Dixon & Hansen op cit note 25 at 611.

<sup>87</sup> Vinje op cit note 9 at 440.

<sup>88</sup> *Ibid.*

<sup>89</sup> Dixon & Hansen op cit note 25 at 611.

<sup>90</sup> Vinje op cit note 42 at 587.

Article 13.1 tried to address these problems by adding a requirement of knowledge directed at infringement. A prerequisite of liability is that the person performing the act knows, or has reasonable grounds to know, that the device or service will be used for or in the course of the unauthorized exercise of any of the author's exclusive rights. So this knowledge requirement focuses on the purpose for which the device or service will be used. The phrase 'knowing or having reasonable grounds to know' has the same meaning as the expression 'knowingly or with reasonable grounds to know' in the enforcement provisions of the TRIPS Agreement.<sup>91</sup>

Vinje<sup>92</sup> argues that the draft article 13.1 suffers the following weakness – it lacks any qualifying language, such as a requirement that the manufacturer knows or has reason to know that the device would be used *primarily* to facilitate infringement. In the absence of such qualifying language, if a manufacturer has reason to believe that only one of its devices will be used to make an unlawful copy, it will be liable. So the proposed knowledge requirement did not adequately address the objections raised to the prohibition of devices.

I doubt whether a provision with a 'knowing or having reason to know' requirement would, in practice, have yielded results meaningfully different from those of the United States proposal. Authors could surely be expected to argue that people intend the natural consequences of their actions. In addition, the commentary to draft article 13 makes clear that the anti-circumvention provision could be employed to challenge the sale of technologies based on predictions about their primary uses,<sup>93</sup> which means that technologies could be challenged before the opportunity arises to see what the primary uses of the product will actually be.<sup>94</sup>

Paragraph (3) of article 13 contains the definition of a 'protection-defeating device'. It describes the characteristics of devices that fall within the scope of the obligations under paragraph (1). To achieve the intended coverage, the phrase 'primary purpose or primary effect of which is to circumvent' has been used rather than the phrase 'specifically designed

---

<sup>91</sup> Note 13.02.

<sup>92</sup> Vinje op cit note 42 at 586.

<sup>93</sup> Draft art 13.2.

<sup>94</sup> Samuelson op cit note 6 at 414.

or adapted to circumvent’.<sup>95</sup>

Although a ‘primary purpose or effect’ test does appear in the definition of a ‘protection-defeating device’, this test applies only to the circumvention itself and not to whether the circumvention is for lawful or unlawful purposes. The test applies to the mere act of circumvention and not to circumvention that primarily facilitates infringement. So a manufacturer would remain liable if the primary purpose or effect of its device was circumvention, even where the manufacturer intended circumvention for lawful purposes only, and where it had no reason to believe that the device would also be used for copyright infringement.<sup>96</sup> If the primary purpose or a primary effect of a device is that it circumvents technological copyright protection measures, such device is prohibited. But a device need not necessarily be primarily designed to circumvent – sometimes a secondary purpose of a device can be to circumvent, and circumvention by means of such a device will no less infringe copyright than will infringement by means of a device the primary purpose of which is to circumvent. The same applies to the effect of a device: only devices with a primary effect of circumvention are proscribed. But a device that can be used to circumvent infringes copyright even if it is not a primary effect of the device that it circumvents technological protection measures. It is interesting to note that the Basic Proposal chose to use ‘primary purpose or effect’ instead of ‘specifically designed to circumvent’. So even if a device were not specifically designed to circumvent, if it has the effect of circumvention, such device would be proscribed. So the prohibition also targets devices not designed specifically only for a circumvention purpose but for broader use.

It was suggested that the primary purpose test of the Basic Proposal should be replaced by a test requiring the device manufacturer to know that the circumvention device had no substantial non-infringing use. Such a test would have protected authors against ‘sham’ defences. Defendants would not have been able to avoid liability by arguing that their devices had some minor function other than circumvention. The ‘no substantial non-infringing use’ test is objective, and would permit a manufacturer to judge for itself, before it engages in significant investment, whether a device capable of circumventing technological protection

---

<sup>95</sup> Note 13.06.

measures had a substantial non-infringing use, and decide on that basis whether to proceed with its investment.<sup>97</sup>

According to Vinje,<sup>98</sup> the adoption of article 13 of the Basic Proposal would have led to the effective elimination of the following copyright exceptions found in Europe: (a) the interoperability provisions of the Computer Programs Directive;<sup>99</sup> (b) exceptions permitting copyright for personal use; (c) exceptions permitting copying for scientific use; and (d) exceptions for educational use.

Some, like Dixon and Hanson,<sup>100</sup> argued that these fears were unfounded. They argued, in the first instance, that formulations such as the ‘primary purpose’ test were narrowly drawn to capture only those devices the main function of which was to facilitate the illegal use and copying of protected works. Secondly, such proposals were intended to preserve the existing balance between authors’ rights and exceptions to those rights (including access to works in the public domain). The proposal was crafted to cover only devices or services that circumvented technological protection measures that prevented or inhibited the infringement of protected rights, and the use of such devices or services in such a way as to exercise those rights, or circumvent such protections without authority. In short, the sort of technological

---

<sup>96</sup> Vinje op cit note 42 at 586.

<sup>97</sup> Vinje op cit note 9 at 436.

<sup>98</sup> Vinje op cit note 42 at 587.

<sup>99</sup> Computer Programs Directive op cit note 63. Article 6 provides that:

‘1. The authorization of the rightholder shall not be required where reproduction of the code and translation of its form within the meaning of Article 4 (a) and (b) are indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs, provided that the following conditions are met:

‘(a) these acts are performed by the licensee or by another person having a right to use a copy of a program, or on their behalf by a person authorized to do so;

‘(b) the information necessary to achieve interoperability has not previously been readily available to the persons referred to in subparagraph (a); and (c) these acts are confined to the parts of the original program which are necessary to achieve interoperability.

‘2. The provisions of paragraph 1 shall not permit the information obtained through its application:

‘(a) to be used for goals other than to achieve the interoperability of the independently created computer program;

‘(b) to be given to others, except when necessary for the interoperability of the independently created computer program; or (c) to be used for the development, production or marketing of a computer program substantially similar in its expression, or for any other act which infringes copyright.

‘3. In accordance with the provisions of the Berne Convention for the protection of Literary and Artistic Works, the provisions of this Article may not be interpreted in such a way as to allow its application to be used in a manner which unreasonably prejudices the right holder's legitimate interests or conflicts with a normal exploitation of the computer program.’

protection provisions under discussion would not have affected the manufacture or use of general purpose devices, tie-up works, or information in the public domain, or altered the existing balance of interests established by the Berne Convention in any way.

According to Marks and Turnbull,<sup>101</sup> the concern that technological protection measures could be used to ‘lock’ works was unfounded. In the first instance, content owners generally depend on the wide public consumption on their works. Protection measures still had to be transparent enough to permit easy access for authorised uses. Secondly, ensuring the availability of works for public purposes, such as libraries and archives, could readily be addressed through licensing arrangements. Restrictions on technological protection measures were not necessary to address these issues. Thirdly, it was unlikely that technological protection measures would be applied to all formats of a work. Fourthly, technological protection measures could actually facilitate certain exceptions to authors’ rights, for example, through ‘copy once’ technology that allowed consumers to make a single copy of a work.

Paragraph (2) of article 13 included a provision relating to remedies against the unlawful acts referred to in paragraph (1). The reason for a special provision for remedies was the fact that the provisions on enforcement in the TRIPS Agreement, which applied according to the proposed article 16, concerned only ‘any act of infringement of intellectual property rights covered by th[e] Agreement’. The obligations in the proposed article 13 were more akin to public law obligations directed at Contracting Parties than to provisions granting ‘intellectual property rights’.<sup>102</sup>

Contracting Parties were free to choose appropriate remedies according to their own legal traditions. The main requirement was that the remedies provided had to be effective and so constitute a deterrent and a sufficient sanction against the prohibited acts.<sup>103</sup>

---

<sup>100</sup> Dixon & Hansen op cit note 25 at 611.

<sup>101</sup> Dean S Marks & Bruce H Turnbull ‘Technical Protection Measures: The Intersection of Technology, Law and Commercial Licences’ [2000] *European Intellectual Property Review* 198 at 202.

<sup>102</sup> Note 13.03.

<sup>103</sup> Note 13.04.

Contracting Parties could design the exact field of application of the provisions envisaged in this article, taking into account the need to avoid legislation that would impede lawful practices and the lawful use of subject matter that was in the public domain. Having regard to differences in legal traditions, Contracting Parties could, in their national legislation, also define the coverage and extent of the liability for any violation of the prohibition enacted in line with paragraph (1).<sup>104</sup>

Not only the Basic Proposal, but also the proposals of the United States and the European Union, prohibited protection defeating devices together with the act of circumvention.<sup>105</sup> Some of the Latin American countries proposed outlawing the act of circumvention itself,<sup>106</sup> which would address the core problem that ultimately will be the most serious for authors.

Copyright law, as found in the Berne Convention and various national instruments, usually prohibits infringing acts, and not devices used for such infringement. The final document, the WCT, which prohibits only the act of circumvention itself, accordingly better suits the WCT's status as a special agreement within the meaning of the Berne Convention.

### **3.3.2 The Final Text of the WCT**

The Preamble to the WCT states that there is a 'need to maintain a balance between the rights of authors and the larger public interest, particularly education, research and access to information, as reflected in the Berne Convention'. Whether the WCT succeeds in maintaining such a balance can be determined only by examining the Article 11 closely.

#### **3.3.2.1 Article 11 of the WCT**

Article 11 of the WCT<sup>107</sup> reads:

---

<sup>104</sup> Note 13.05.

<sup>105</sup> Dixon & Hansen op cit note 25 at 610-611.

<sup>106</sup> WIPO, Questions Concerning a Possible Protocol to the Berne Convention: Proposal of Argentina, BCP/CE/V/7 (6 September 1995) at 3 to 4.

<sup>107</sup> Fitzpatrick op cit note 9 at 222.

‘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.’

There are no agreed statements in respect of this article.

Article 11 prohibits the circumvention of effective technological protection measures. The prohibition in article 11 strikes at the act of circumvention, unlike the prohibition proposed in draft article 13 of the Basic Proposal that concerned not only the act of circumvention itself, but also the importation, manufacture, or distribution of devices used to circumvent technological protection. Not only was the act of circumvention itself (‘the performance of services having the same effect’) proposed to be prohibited, but also the offer of such services. The draft article 13 of the Basic Proposal thus effectively listed the acts that could result in circumvention, whereas article 11 of the WCT merely prohibits *any* act that can result in circumvention. Unlike the draft article 13, article 11 is formulated in a broad and neutral way, aimed more at the desired result than on how to achieve it.

Since the draft article 13 listed the various acts that could result in circumvention, it necessarily included a prohibition on dealing with devices that could be used for circumvention. The anti-circumvention language of article 11, by contrast, does not state expressly whether its prohibition extends to devices, too.

The question, then, is whether the prohibition in the WCT should be read to be aimed only at circumvention conduct, or whether it should extend also to devices used for circumvention.

On the one hand, it is argued that a ‘conduct alone’ approach would be insufficient, because the acts of circumvention will usually be carried out by private individuals in their homes or offices, where enforcement will be much more difficult, amongst other things, because of objections based on considerations of privacy. But the results of circumvention conduct, such as a software utility program that ‘hacks’ a copy protection measure, may be made public, in

contrast to the conduct leading up to the cracking of the protection system which is usually private. If legislation covers only the act of circumvention itself, which is usually carried out in private, it will not provide adequate legal protection and effective remedies against such acts which would continue uncontrolled in spite of treaty obligations.<sup>108</sup>

Ginsberg<sup>109</sup> supports the argument that the text of the WCT should not be limited to the act of circumvention. Since circumvention can only be accomplished by means of devices, machines, or computer programs, protection against circumvention would not be 'adequate and effective' if only the acts of circumvention were covered.

Ficsor<sup>110</sup> is also of the opinion that countries will discharge their article 11 obligations only by prohibiting, inter alia, dealings with circumvention devices. He regards dealings with circumvention devices and tools as 'preparatory activities' that render circumvention possible. He sees the prohibition as not being directed at the devices themselves, but at the acts that pave the way for the infringer to circumvent the protection measures. Such interpretation means, however, that article 11 prohibits not only circumvention conduct but also circumvention devices.

The United States of America likewise interprets article 11 to include a prohibition on circumvention devices. The Global Business Dialogue on Electronic Commerce<sup>111</sup> (the 'GBDe') has also recommended that national legislation implementing the WCT should 'prohibit harmful circumvention related activities by regulating both conduct and devices, while providing appropriate exceptions . . . that would maintain the overall balance between rightholders and users'.<sup>112</sup>

On the other hand, one can argue that the WCT is part of the international copyright regime,

---

<sup>108</sup> Ficsor op cit note 5 para C11.12 at 549; Marks & Turnbull op cit note 101 at 201.

<sup>109</sup> Jane C Ginsberg 'Copyright Legislation for the "Digital Millennium"' (1999) 23 *Columbia - VLA Journal of Law and the Arts* 137 at 138.

<sup>110</sup> Ficsor op cit note 5 para C11.12 at 550.

<sup>111</sup> The Global Business Dialogue on Electronic Commerce (the 'GBDe') constitutes a worldwide collaboration among companies engaged in the field of electronic commerce. Several hundred companies and trade associations have participated in the GBDe consultation process; the representation is both geographically and sectorally diverse (Marks & Turnbull op cit note 101 at 200n 2).

<sup>112</sup> Marks & Turnbull op cit note 101 at 201.

and that, in line with the general principles of copyright law, only circumvention conduct, and not also circumvention devices, should be prohibited.<sup>113</sup> Even if Ficsor's argument that the prohibition should extend to preparatory acts were to be accepted, this interpretation is still not in line with the general principles of copyright law – there is no prohibition on 'preparatory activities' in copyright law. In any event, the result of this argument would be that the prohibition on the act of circumvention in article 11 would be extended to include a prohibition on devices, like the prohibition in the draft article 13 of the Basic Proposal.

A further problem with prohibiting circumvention devices would be to determine which devices should be prohibited. When a legislator prohibits a service or device, setting the boundaries as to exactly what device or service is prohibited is not simple. The cases at the ends of the spectrum are relatively straightforward. So-called black boxes that serve solely, for example, to decrypt television signals without authorization, or to strip out copy protection measures, are clearly illegal. Personal computers, at the other end of the spectrum, generally serve overwhelmingly legitimate purposes and functions but are sometimes put to illicit use, such as to crack copy protection measures for software. The problem is where to draw the line between these two extremes.<sup>114</sup>

The WCT does not expressly preclude Contracting Parties from adopting device focused prohibitions. Whether the prohibition on circumvention relates to conduct only or to conduct and devices, will accordingly have to be answered by domestic legislators when they implement the treaty provisions.

Article 11 expressly states that the only technological protection measures that are protected are those '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.'

Vinje<sup>115</sup> states that, by focussing on acts facilitating *infringement*, the WCT assures that the

---

<sup>113</sup> Vinje op cit note 9 at 434.

<sup>114</sup> Marks & Turnbull op cit note 101 at 201.

<sup>115</sup> Vinje op cit note 63 at 201.

sphere of application of the circumvention provision corresponds to that of copyright infringement, which preserves the copyright balance. This will also have the effect that anyone who circumvents a technological protection measure to make unauthorized copies of a work breaches not only copyright law, but also the prohibition on circumvention for the purposes of infringement.<sup>116</sup> So such a person incurs liability on two fronts – copyright infringement, and falling foul of the circumvention prohibition.

This wording of article 11 tries to address some of the objections raised against the draft article 13 of the Basic Proposal – that the draft article 13 could extend copyright protection to works not protected by copyright, or extend the term of protection of copyright works indefinitely. Under the draft article 13, the circumvention of measures used to protect works that enjoyed no copyright protection, or where the use of the works was authorized by the author or permitted by law, were not prohibited. So a person, who circumvents a technological protection measure for purposes of engaging in acts permitted by law, would not have been liable for copyright infringement nor for contravening the circumvention prohibition.<sup>117</sup>

It has been argued that a prohibition on circumvention *for purposes of infringement* adds nothing to existing law – the author can in any event sue for copyright infringement. However, as Vinje<sup>118</sup> correctly remarks, damages for circumvention would be awarded in addition to those awarded for copyright infringement. The circumvention prohibition can, therefore, provide a significant deterrent to copyright infringement, especially where additional criminal penalties are imposed for circumvention, or where circumvention might be taken into account in determining whether a copyright infringement should be deemed a criminal offence.

Article 11 does not define the type of technological measure that it protects. But it is generally accepted<sup>119</sup> that article 11 requires protection for both access control and copy

---

<sup>116</sup> *Idem* at 197.

<sup>117</sup> *Ibid.*

<sup>118</sup> *Idem* at 198.

<sup>119</sup> See, *inter alia*, <<http://www.ifpi.org/site-content/library/wipo%20treaties%20-%20technical%20measures.pdf>> (visited on 5 April 2002).

control technologies. Neither the Berne Convention nor the WCT accords an author an exclusive right to authorize access to a work protected by copyright. Does this mean that article 11 indirectly creates an access right? I will address this question in Chapter 7.

Article 11 proscribes the ‘circumvention of effective technological measures’. The circumvention of effective protection measures that are not technological is not affected. The draft article 13 of the Basic Proposal merely referred to a ‘protection-defeating device’, and defined such a device as ‘any device, product or component incorporated into a device or product, the primary purpose or primary effect of which is to circumvent any process, treatment, mechanism or system that prevents or inhibits any of the acts covered by the rights under this Treaty.’ The use of the words ‘which is to circumvent any process, treatment, mechanism or system’ confirmed a broader application: it was not limited to a technological process, treatment, mechanism, or system, but aimed at any process, treatment, mechanism, or system as long as the said process, et cetera prevented or inhibited any of the acts covered by the rights under the proposed treaty. However, the addition of a reference to the purpose or effect of the device limited the ambit of the draft article 13. Article 11, therefore, limits the envisaged protection to technological protection measures. The term ‘technological’ is not defined. I prefer this to the inclusion of a definition, because the rapid and ever-changing technology can render such a definition obsolete very soon. If definitions were to be given for a term such as ‘circumvention’, they should be functional rather than ‘technology-specific’ in order to avoid technical obsolescence.<sup>120</sup>

A technological protection measure will be protected only as long as it *effectively* restricts the use of the content in any manner. There is no threshold standard of sophistication or security, as long as the technological protection measure effectively protects the work.<sup>121</sup> However, as there is no threshold, when will a technological protection measure be deemed to be ‘effective’? And will the fact that a technological protection measure has actually been circumvented, or the availability of a circumvention device, affect whether a device is deemed to be ‘effective’?

---

<sup>120</sup> Ficsor op cit note 5 at 549.

<sup>121</sup> See <<http://www.ifpi.org/site-content/library/wipo%20treaties%20-%20technical%20measures.pdf>> (visited on 5 April 2002).

The IFPI<sup>122</sup> states that technological protection measures that have been subject to attack are the ones that most need protection. So the fact that a technological protection measure has actually been circumvented does not affect its effectiveness. Ficsor<sup>123</sup> agrees that the term ‘effective’ cannot be construed to connote that, if a technological protection measure can be circumvented, it cannot be regarded as ‘effective’. The objective of the prohibition is indeed to guarantee protection against acts of circumvention which, by definition, is also presumed to be possible in case of an ‘effective’ technological measure.

Unlike its predecessor in the Basic Proposal, article 11 does not expressly require ‘knowledge’ from the circumventor. However, it seems that the ‘effectiveness’ requirement imparts a knowledge requirement – if a technological protection measure is not effective, a user of a work cannot gather that the work is actually protected. So only where a technological protection measure is effective can a user be expected to know that it is protected, and that the circumvention of the protection measure is prohibited.

Although the aim of the WCT is to provide copyright protection in the digital environment, the addition of the word ‘technological’ to the phrase is not welcome – not all protection measures used in the digital world are technological. Where, for example, a digital work is protected by a contractual barrier, the circumvention of such barrier would not be proscribed by article 11 – a contractual protection measure is not a technological protection measure.

Article 11 expressly states that the technological measures should be ‘used by authors’. The WCT leaves it to authors to decide whether or not to apply technological protection measures, and if they do, what kind of measures. However, once such measures are applied, the obligation to provide ‘adequate legal protection and effective legal remedies’ against their circumvention comes into existence.<sup>124</sup>

Finally, a brief remark: the circumvention of technological protection measures is distinct

---

<sup>122</sup> Ibid.

<sup>123</sup> Ficsor op cit note 5 at 545.

<sup>124</sup> Idem at 547.

from copyright infringement. The violation occurs when the circumvention takes place. It is not necessary to prove that the circumvention actually resulted in copyright infringement.<sup>125</sup> However, since only those protection measures used to protect copyright works are protected, circumvention is usually followed by copyright infringement.

To summarize: technological protection measures must meet certain requirements before their circumvention is prohibited by article 11 of the WCT: such measure must be *used by an author* in exercising his or her exclusive rights in terms of the Berne Convention or the WCT; the measure must restrict only *infringing* acts; the measure is protected as long as it *effectively* restricts use of the work in any manner; and the measure must be *technological*.

### 3.3.2.2 Limiting Article 11

National laws, generally, provide for exceptions to the rights of authors, such as fair use. The Berne Convention sets out the parameters for the exceptions to these rights. Generally, these exceptions may be provided for only ‘in certain special cases that do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interest of the author’.<sup>126</sup>

Article 11 does not contain any provision obliging Contracting Parties to provide exceptions to the circumvention prohibition. Article 10 of the WCT deals with exceptions and limitations. It reads as follows:

“(1) Contracting Parties may, in their national legislation, provide for limitations of or exceptions to the rights granted to authors of literary and artistic works under this Treaty in certain special cases that do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the author.

(2) Contracting Parties shall, when applying the Berne Convention, confine any limitations of or exceptions to rights provided for therein to certain special cases that

---

<sup>125</sup> Ginsberg op cit note 109 at 138.

<sup>126</sup> See arts 9(2), 10 and 10bis of the Berne Convention, art 10 of the WCT and art 16 of the WPPT.

do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the author.”

Article 10, then, allows Contracting Parties to carry forward and appropriately extend into the digital environment exceptions in their national laws that have been considered acceptable under the Berne Convention. It is interesting to note that there is no obligation on Contracting Parties to provide for exceptions and limitations. The wording of article 10.1 is expressly permissive. The Agreed Statement Concerning Article 10 clearly states that ‘. . . the provisions of Article 10 *permit* Contracting Parties to carry forward . . . limitations and exceptions. . .’ (emphasis added) that are appropriate in the digital environment.<sup>127</sup> Article 10 accordingly allows Contracting Parties to provide for exceptions, but it does not compel them to do so.

Article 10 expressly states that the exceptions and limitations apply only to the *rights* granted to authors. Article 11 of the WCT does not, however, confer any right but merely creates a type of infringement. So the WCT does not specifically provide for exceptions to the obligation to provide adequate legal protection against circumvention.<sup>128</sup> The only mandate to maintain copyright exceptions is in the preamble to the WCT.

But this does not mean that article 10 is of no importance to the interpretation of article 11. Article 11 prohibits the circumvention of technological protection measures where such circumvention would lead to an unauthorized (and hence illegal) act. The act is illegal where it infringes an author’s exclusive rights of authorization. So article 11 protects an author’s exclusive rights. These rights themselves are limited by article 10.

Article 10 comes into play to determine whether the intended act, after the technological protection measure has been circumvented, is authorized and hence legal. Where the intended

---

<sup>127</sup> Article 10; Agreed Statement Concerning Article 10.

<sup>128</sup> According to the IFPI, the problem with allowing exceptions to the protection of technological protection measures is similar to allowing someone to break the lock on a safe. Anyone then can get in, for any purpose. Allowing hacking or circumvention devices weaken the overall robustness of the technological protection measures. Carried too far, this can make use of technological protection measures pointless and investment in equipment and technologies worthless (<<http://www.ifpi.org/site-content/library/wipo%20treaties%20-%20technical%20measures.pdf>> (visited on 5 April 2002)).

act or use is an instance where the exercising of rights is permitted, then the circumvention of the protection measure does not amount to copyright infringement.

Such an interpretation addresses the concern that authors will use technological protection measures to ‘lock up’ their works and prevent users from exercising their legitimate exceptions to the authors’ rights.

As I shall show below, national legislators have, in their implementation of article 11, also provided for exceptions. Vinje<sup>129</sup> even believes that these exceptions should be mandatory. But there is no legal basis for obliging Contracting Parties to provide for exceptions to the circumvention prohibition, because no such obligation is stated in the WCT.

### **3.3.2.3 Enforcing Article 11**

Effective legal remedies to enforce article 11 are of great importance, because action against the circumvention of technological protection measures must be sufficiently speedy, efficient, and deterrent to future circumventors in order to counter the great incentive to hackers to circumvent technological protection measures and appropriate content.

The draft article 13.2 of the Basic Proposal contained its own enforcement provision:

‘Contracting Parties shall provide for appropriate and effective remedies against the unlawful acts referred to in paragraph (1)’.

The Basic Proposal thus sought to deal with the enforcement of article 13 separately from the enforcement of the rest of the proposed treaty. The reason for a special provision relating to remedies was that the enforcement provisions in the TRIPS Agreement, which were to apply according to the proposed article 16, concerned only ‘any act of infringement of intellectual property rights covered by this Agreement’. The obligations established in the proposed article 13 were more like public law obligations directed at Contracting Parties than like

---

<sup>129</sup> Vinje op cit note 63 at 196.

provisions granting ‘intellectual property rights’.<sup>130</sup>

Article 11 of the WCT does not contain a similar provision. Accordingly, unlike its predecessor, article 11 must be enforced similarly to the rest of the Treaty. The general provisions on the enforcement of rights are contained in article 14 of the WCT. When discussing the enforcement of article 11, the draft article 16 of the Basic Proposal and article 14 of the WCT are both relevant.

The enforcement procedures envisaged in the draft article 16 of the Basic Proposal<sup>131</sup> provided two alternative formulations – either transposing<sup>132</sup> the TRIPS Agreement enforcement text<sup>133</sup> to the new instrument, or incorporating these provisions by reference.<sup>134</sup> Most of the delegates preferred incorporating the TRIPS Agreement provisions into the new instrument in some or other form.<sup>135</sup> At earlier meetings of the Committee of Experts, the United States of America was the principal opponent of including enforcement provisions in the new instrument. Its delegates expressed the fear that doing so might lead to conflicting interpretations of what should be identical norms. They argued that the TRIPS Agreement text was already binding on almost all Berne Union members.<sup>136</sup>

In the end, neither approach mooted in the Basic Proposal was adopted. The second sentence of article 1.1 of the WCT states that ‘[t]his Treaty shall not have any connection with treaties other than the Berne Convention, nor shall it prejudice any rights and obligations under any other treaties’.<sup>137</sup> So the WCT has no formal connection to TRIPS. Article 14 of the WCT, which contains the provisions on the enforcement of rights, states that it is left to Contracting Parties to adopt, in accordance with their legal systems, the measures necessary to ensure the application of this treaty.<sup>138</sup> Mort<sup>139</sup> has argued that these two provisions constitute a

---

<sup>130</sup> Note 13.03 on Article 13.

<sup>131</sup> Article 16 of the Basic Proposal op cit note 14.

<sup>132</sup> Article 16, Alternative A of the Basic Proposal op cit note 14.

<sup>133</sup> TRIPS, Articles 41 to 61 (‘Enforcement of Intellectual Property Rights’).

<sup>134</sup> Article 16, Alternative B of the Basic Proposal op cit note 14. See also Mort op cit note 1 at 202.

<sup>135</sup> TRIPS, Articles 41 to 61 (‘Enforcement of Intellectual Property Rights’); Mort op cit note 1 at 202.

<sup>136</sup> Dixon & Hansen op cit note 25 at 611.

<sup>137</sup> Fisor op cit note 2 at 201.

<sup>138</sup> Article 14.1 of WCT.

<sup>139</sup> Mort op cit note 1 at 202.

‘stunning rejection’ of the enforcement provisions in the TRIPS Agreement, considering that even WIPO officials admit ‘that there would be huge technical problems in enforcing copyright legislation’ because national liability standards differ. As a result, in order for the enforcement guidelines in the TRIPS Agreement to apply, the WTO must integrate the WCT into the substantive provisions of the TRIPS Agreement.

Article 14 of the WCT reads as follows:

‘(1) Contracting Parties undertake to adopt, in accordance with their legal systems, the measures necessary to ensure the application of this Treaty.

‘(2) Contracting Parties shall ensure that enforcement procedures are available under their law so as to permit effective action against any act of infringement of rights covered by this Treaty, including expeditious remedies to prevent infringements and remedies which constitute a deterrent to further infringements.’

Paragraph (1) of article 14 is a close adaptation of article 36(1) of the Berne Convention. Paragraph (2) is a close adaptation of the first sentence of article 4.1 of the TRIPS Agreement. Article 14 does not indicate whether these remedies should include criminal liability, and no minimum civil damages or criminal fines are laid down.<sup>140</sup>

The draft article 13.2 of the Basic Proposal<sup>141</sup> stated that ‘Contracting Parties shall provide for appropriate and effective remedies against the unlawful acts referred to in paragraph (1).’ According to the Notes on Article 13,<sup>142</sup> this meant that ‘Contracting Parties are free to choose appropriate remedies according to their own legal traditions’. Although this proposal dealt exclusively with remedies against circumvention, this provision was added unaltered to article 14.1 of the WCT, which contains the general enforcement provisions of the WCT. Article 14.2 of the WCT contains the only performance condition for these remedies – they should be effective.

---

<sup>140</sup> Fisor op cit note 2 at 219.

<sup>141</sup> Article 13 of the Basic Proposal op cit note 14 deals with ‘Obligations concerning Technological Measures’.

<sup>142</sup> Note 13.04.

The WCT, like the Berne Convention,<sup>143</sup> expects of Contracting Parties to provide their own enforcement and sanction procedures. Article 36 of the Berne Convention, on the enforcement of rights, does not form part of the WCT, since WCT Contracting Parties are compelled only to comply with articles 1 to 21 and the Appendix of the Berne Convention. However, since the WCT is a special agreement within the meaning of article 20 of the Berne Convention (it stipulates that such special agreement may only provide ‘authors more extensive rights than those granted by the Convention’), the enforcement measures adopted by the Contracting Parties should not be any lower than those available for copyright infringement under the Berne Convention.<sup>144</sup> This implies that effective legal remedies should at least be the same as the existing remedies in the different copyright systems of the Contracting Parties, and that it should include both criminal law sanctions and civil law remedies. Criminal penalties should permit fines and prison terms in appropriate cases. To serve as a deterrent, civil law should allow fast and efficient preliminary proceedings, injunctive relief, the payment of damages (including statutory damages), and the obligation to co-operate in neutralizing harm already caused. It is also argued that for the enforcement provisions to be effective, remedies should also allow tracing, seizure, retention, and destruction of physical circumvention devices and intangible software, and information used to circumvent protection measures.<sup>145</sup>

### **3.4 Objections to the WCT**

Response to the WCT was positive. However, despite the fact that the WCT tries to address many of the problems created by digitization, it is not without deficiencies. Many of these will also impact on the effectiveness of article 11.

The greatest objection to the WCT is that it relies entirely on old notions of copyright protection, in particular, on national implementation.

---

<sup>143</sup> Article 36.

<sup>144</sup> See also <<http://www.ifpi.org/site-content/library/wipo%20treaties%20-%20technical%20measures.pdf>> (visited on 5 April 2002).

<sup>145</sup> Ibid.

The preamble to the WCT states that the Contracting Parties desire to ‘. . . develop and maintain the protection of the rights of authors in their literary and artistic works in a manner as effective and uniform as possible. . .’ The WCT did achieve uniformity. It is formulated in general terms and leaves it to national legislators to go further and in greater detail offer efficient protection for technological measures.<sup>146</sup> It directs national legislators as to some minimum standards that their domestic copyright laws must incorporate.<sup>147</sup> So the effectiveness of the treaty provisions is subject to how they will be translated in national legislation.<sup>148</sup> As each country is entitled to legislate treaty terms with its own distinctive twists, countless differences will remain in copyright laws as one crosses national borders.<sup>149</sup> The retention of a minimum standards type regime in the WCT may actually inhibit the development of a global marketplace, because of the intrinsic difficulties caused by applying different national standards to a technology that does not acknowledge physical and geographic borders.<sup>150</sup>

In addition to the scope of rights differing from one country to another, the scope of the exceptions and limitations also differ. The WCT clearly countenances various exceptions and limitations, and allows each country discretion as to the manner of its implementation.<sup>151</sup>

Inequalities in domestic legislation could not only make enforcement of the WCT difficult, but could also stifle the growth of global information networks such as the Internet as a means of commerce.<sup>152</sup>

The WCT rejects the WTO’s dispute settlement system and the enforcement procedures of the TRIPS Agreement.<sup>153</sup> In the event of crossborder disputes, authors will have to rely on traditional enforcement procedures. A hallmark of copyright protection has always been suit within the country of infringement. This continues under the WCT; it does not obliterate

---

<sup>146</sup> Fisor op cit note 2 at 216-217.

<sup>147</sup> Nimmer op cit note 20 at 7.

<sup>148</sup> Fitzpatrick op cit note 9 at 222.

<sup>149</sup> Nimmer op cit note 20 at 8.

<sup>150</sup> Mort op cit note 1 at 204.

<sup>151</sup> Nimmer op cit note 20 at 8.

<sup>152</sup> Mort op cit note 1 at 216.

<sup>153</sup> Idem at 217.

national boundaries.<sup>154</sup> Suit within the country of infringement can lead to very high litigation costs, as infringement in the context of the Internet can take place simultaneously in several legal systems, often with widely differing standards.<sup>155</sup> Suit within the country of infringement can also lead to business and legal entities choosing their forum based on the vagaries of procedure here and there. An international forum could avoid this type of needless side-tracking.<sup>156</sup>

Only Contracting Parties are bound by the WCT. There are presently 61 signatories to the WCT, all of which have not yet ratified the provisions of the treaty.<sup>157</sup> However, once copyright works appear on Internet, they can be accessed from anywhere in the world, including from non-Contracting Parties of the WCT. These countries are not compelled to provide protection for technological protection measures.

### **3.5 Conclusion**

The WCT establishes, despite its flaws, an international consensus on the application of copyright principles to digital technologies. This can serve as the foundation for further legal development. However, the Treaty requires near universal acceptance and participation in order to be truly effective. The only viable means for ensuring this kind of participation is to integrate the WCT into the TRIPS Agreement so that it can benefit from the disciplines of the WTO and its Dispute Settlement Understanding.<sup>158</sup>

In the next two chapters, I shall look at how the general prohibition against the circumvention of technological protection measures of the WCT was implemented in the United States of America and the European Union. Thereafter I will discuss current South African legislation. Traditionally, copyright protects an author's reproduction right. However, the adoption of article 11 of the WCT created a new right in copyright law - an access right. In the following chapter I shall then discuss this new exclusive right before I will make certain suggestions

---

<sup>154</sup> Nimmer op cit note 20 at 8.

<sup>155</sup> Mort op cit note 1 at 216.

<sup>156</sup> Nimmer op cit note 20 at 7.

<sup>157</sup> The list of signatories is available at [http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty\\_id=16](http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=16) (visited on 11 January 2007).

about how the prohibition against the circumvention of technological protection measures should be incorporated into South African law.

---

<sup>158</sup> Mort op cit note 1 at 221.

## CHAPTER 4: THE UNITED STATES OF AMERICA

“I wish I hadn’t cried so much!” said Alice, as she swam about, trying to find her way out. “I shall be punished for it now, I suppose, by being drowned in my own tears! That *will* be a queer thing, to be sure! However, everything is queer to-day.”

LEWIS CARROL

*Alice’s Adventures in Wonderland*

### 4.1 Introduction

In the United States, copyright works were traditionally protected only to the extent necessary to stimulate authors<sup>1</sup> to create more works. This philosophical approach is enshrined in the Copyright Clause<sup>2</sup> of the Constitution which authorizes Congress ‘[t]o promote the progress of science and the useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries’.

Kurtz<sup>3</sup> summarizes the American position thus:

‘Authors are rewarded, but with the ultimate aim of stimulating artistic creativity and making literature, music and other arts broadly available to the public.’

So copyright protection exists solely to provide economic incentives for the production of useful works.<sup>4</sup> This incentive approach appears from the following dictum in *Sony Corporation of America v Universal City Studios Inc.*<sup>5</sup>

‘The monopoly privileges that Congress may authorize are neither unlimited nor

---

<sup>1</sup> United States copyright legislation uses the term ‘copyright owner’ rather than ‘author’. However, for sake of uniformity, I shall use the term ‘author’ in this chapter.

<sup>2</sup> United States Constitution art I § 8 cl 8.

<sup>3</sup> LA Kurtz ‘Copyright and the National Information Infrastructure in the United States’ [1996] *European Intellectual Property Review* 120 at 121, citing *Twentieth Century Music v Aiken* 422 US 151 (1975) at 156.

<sup>4</sup> Alfred C Yen ‘Restoring the Natural Law: Copyright as Labor and Possession’ (1990) 51 *Ohio State Law Journal* 517.

primarily designed to provide a special private benefit. Rather, the limited grant is a means by which an important public purpose may be achieved. *It is intended to motivate the creative activity of authors and inventors by the provision of a special reward, and to allow the public access to the products of their genius after the limited period of exclusive control has expired.*'

And in *Mazer v Stein*:<sup>6</sup>

'The economic philosophy behind the clause empowering Congress to grant patents and copyrights is the conviction that encouragement of individual effort by personal gain is the best way to advance public welfare through the talents of authors and inventors in "Science and useful Arts".'<sup>7</sup>

However, as I shall show below, the United States implemented the prohibition on the circumvention of technological protection measures in article 11 of the WIPO Copyright Treaty (WCT) in such a way that authors in the digital world enjoy protection far greater than that needed to stimulate creativity.<sup>8</sup> This deviation from the incentive approach can be attributed to trade interests.<sup>9</sup> The United States is home to a major the film industry, a major recording industry, and Silicon Valley (software), and it hosts many Internet web sites.<sup>10</sup> It is the world's largest exporter of copyright works<sup>11</sup> and so stands to receive increased revenue from enhanced copyright protection.<sup>12</sup> But increased revenue is not the only advantage to be gained from stronger protection. It has been argued that stronger protection would protect

---

<sup>5</sup> 464 US 417 (1984) at 429 (emphasis added).

<sup>6</sup> 347 US 201 (1954) at 219.

<sup>7</sup> See also *Quinto v Legal Times of Washington Inc* 511 F Supp 579 (DDC 1981); *Diamond v Am-Law Publishing Corp* 745 F 2d 142 (2d Cir 1984).

<sup>8</sup> Simon Fitzpatrick 'Copyright Imbalance: U.S. and Australian Responses to the WIPO Digital Copyright Treaty' [2000] *European Intellectual Property Review* 214 at 222, 223, 224 and 228; Pamela Samuelson 'Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised' (1999) 14 *Berkeley Technology Law Journal* 519 at 521.

<sup>9</sup> Fitzpatrick op cit note 8 at 228.

<sup>10</sup> David Nimmer 'Time and Space' (1998) 38 *IDEA: The Journal of Law and Technology* 501 at 509.

<sup>11</sup> Thomas Vinje 'Copyright Imperilled?' [1999] *European Intellectual Property Review* 192 at 202.

<sup>12</sup> The copyright industries in the United States are its most important exporters. The international sale and export of films, videos, literature, music, and software exceed that of automobiles and agricultural products. Unfortunately, it is estimated that these industries also lose billions of dollars in international revenue annually (Bonnie JK Richardson, *Congressional Testimony*, 21 May 1998, available in 1998 WL 12760304 at ¶ 4, cited by Carolyn Andrepont 'Digital Millennium Copyright Act: Copyright Protections for the Digital Age' (1999) 9

American ideas and industry and create more jobs, and that the intellectual property-based industries would restore the United States to a positive trade balance with the rest of the world.<sup>13</sup>

Unfortunately, not all consequences of such stronger protection are positive, nor are they confined to the United States. In the first instance, although stronger protection benefits the United States as a copyright exporting country, it is detrimental to copyright importing countries. The reason for this is that stronger copyright protection necessarily comes with fewer user privileges, also for copyright importing countries. Secondly, even users outside United States borders may be subjected to the stronger copyright protection afforded by United States legislation. This is because the private international law rules of the United States appear to be more liberal than, for example, those of the United Kingdom. As a result of its more liberal rules, a United States court can assume personal jurisdiction over extra-territorial defendants in cyber litigation and so subject them to the stronger United States copyright protection.<sup>14</sup> Thirdly, the pro-author bias of United States copyright could serve as model for other countries. It has been suggested, in fact, that one reason for the relatively quick implementation of the WCT in the United States was so that its legislation could serve as a template for other.<sup>15</sup> So United States authors were 'primed to win stronger digital copyright protections around the globe as Congress's actions will likely be mimicked when other nations ratify the treaties'.<sup>16</sup>

However, not everyone in the United States was in favour of stronger copyright protection, despite its many economic advantages. Two main objections were voiced. In the first instance, stronger protection was likely to harm innovation and competition in the digital economic sector. Secondly, stronger protection may curtail users' abilities to make fair or other non-infringing uses of copyright works.<sup>17</sup>

---

*De Paul-LCA Journal of Art and Entertainment Law* 397 at 405; see also Fitzpatrick op cit note 8 at 222).

<sup>13</sup> Fitzpatrick op cit note 8 at 224 and 227.

<sup>14</sup> *Idem* at 227.

<sup>15</sup> Andrepont op cit note 12 and 412; Samuelson op cit note 8 at 537.

<sup>16</sup> J Litman 'Digital Copyright and Information Policy', <<http://www.msen.com/~litman/carip.html>>, cited by Fitzpatrick op cit note 8 at 227.

<sup>17</sup> Fitzpatrick op cit note 8 at 224, 227.

It was feared, then, that the privileges enjoyed by copyright users in the United States, and in the rest of the world, were at risk of drowning in the sea of the new circumvention prohibition. Was this risk real? To answer this question, I shall examine the preparation of United States legislation regulating copyright in the digital world. I shall then discuss the implementation of the WCT by the Digital Millennium Copyright Act<sup>18</sup> (DMCA), especially the prohibition on circumvention and circumvention devices, the responsibility of equipment manufacturers, the obligations of authors, the limitations and exceptions to the prohibitions, remedies, and the objections to the implementation of the circumvention prohibition.

#### **4.2 Preparations for Law Making in the Digital Era**

In 1993, President Clinton formed the Information Infrastructure Task Force (IITF). The principal goal of the IITF was to make policy recommendations that would promote the optimal development of the emerging information infrastructure.<sup>19</sup> The IITF established a number of working groups to focus on specific policy areas. One of them was the Working Group on Intellectual Property Rights (the 'Working Group'), chaired by Bruce Lehman, then Assistant Secretary of Commerce and Commissioner of Patents and Trademarks.<sup>20</sup> The primary goal of the Working Group was to consider copyright law in the light of new technology.<sup>21</sup> The copyright objectives of the Clinton administration, according to its Internet policy report, *A Framework for Global Electronic Commerce*, included ensuring that US trading partners adopt, implement, and enforce laws and regulations to protect copyright works disseminated over the Internet.<sup>22</sup>

The recommendations of the Working Group, especially those regarding technological protection measures, are reflected in the Green Paper,<sup>23</sup> the White Paper,<sup>24</sup> and the United

---

<sup>18</sup> L No 105-304, 112 Stat 2860 (28 October 1998).

<sup>19</sup> Pamela Samuelson 'The U.S. Digital Agenda at WIPO' (1997) 37 *Virginia Journal of International Law* 369 at 379.

<sup>20</sup> June M Besek 'Anti-Circumvention Laws and Copyright: A Report from the Kernochan Center for Law, Media and the Arts' (2004) 27 *Columbia Journal of Law & the Arts* 385 at 400.

<sup>21</sup> Eric D Keller 'Scan Now, Pay Later: Copyright Infringement in Digital Document Storage' (2000) 26 *The Journal of Corporation Law* 177 at 189.

<sup>22</sup> Mark Felsenthal & Angela Droite 'Administration Outlines Objectives for Global Internet Policy' (1997) 14(28) *International Trade Reporter (BNA)* 1179.

<sup>23</sup> Information Infrastructure Task Force Intellectual Property and the National Information Infrastructure: *A Preliminary Draft of the Report of the Working Group on Intellectual Property Rights: The Green Paper* (July

States Proposal for the Protocol to the Berne Convention.

#### 4.2.1 The Green Paper

In July 1994, the Working Group issued a 140-page preliminary draft report (or ‘Green Paper’).<sup>25</sup> It focussed principally on copyright law and its application to the National Information Infrastructure.<sup>26</sup>

Chapter II, headed ‘Technology’, deals with the technological aspects of copyright protection. Its introduction states that technological measures can be used to protect works against copyright infringement, to authenticate the integrity of the works, and to manage and licence the rights in such works.<sup>27</sup>

Chapter IV, headed ‘Preliminary Findings and Recommendations’, includes a recommendation for the adoption of the following new section 512 in the Copyright Act of 1976:<sup>28</sup>

‘No person shall import, manufacture, or distribute any device, product, or component incorporated into a device or product, or offer or perform any service, the primary purpose or effect of which is to avoid, bypass, remove, deactivate, or otherwise circumvent, without authority of the copyright owner or the law, any process, treatment, mechanism or system which prevents or inhibits the exercise of any of these exclusive rights under section 106.’<sup>29</sup>

So the United States contemplated the protection of technological protection measures even before the international community saw the need to include such protection in an

---

1994).

<sup>24</sup> Information Infrastructure Task Force: *The Report of the Working Group on Intellectual Property Rights, Intellectual Property and the National Information Infrastructure: The White Paper* (Sept 1995).

<sup>25</sup> The Green Paper op cit note 23.

<sup>26</sup> Kurtz op cit note 3 at 120.

<sup>27</sup> Mihály Ficsor *The Law of Copyright and the Internet: The 1996 WIPO Treaties, Their Interpretation and Implementation* (2002) para 6.24 at 373.

<sup>28</sup> 17 USC §§ 101-1205.

<sup>29</sup> The Green Paper op cit note 23 at 126.

international treaty.

#### **4.2.2 The White Paper**

The final report of the Working Group is the White Paper.<sup>30</sup> It contains the results of the debates about the amendments proposed in the Green Paper.

Essentially, three concerns had been raised against the anti-circumvention recommendations in the Green Paper. The White Paper addresses these concerns.

The first concern was that the prohibition of circumvention devices could be incompatible with fair use. According to the authors of the White Paper this concern is unfounded – the fair use doctrine does not require an author to allow or facilitate unauthorized access or use of her work.

‘Otherwise copyright owners could withhold works from publication; movie theatres could not charge admission or prevent audio or video recording; museums could not require entry fees or prohibit the taking of photographs. Indeed if the provision of access and the ability to make fair use of works protected by copyright were required by copyright owners - or an affirmative right of the public – even passwords for access to computer databases would be considered illegal.’<sup>31</sup>

Furthermore, a circumvention device used for a legal purpose such as fair use, would not violate the prohibition, as such a device would fall under the ‘authorized by law’ exception.<sup>32</sup> I shall discuss the question as to whether such an exception will indeed allow fair and other legitimate uses in more detail below.

The second concern was that the proposed prohibition could effectively be used indirectly to

---

<sup>30</sup> See also Christine Jeanneret ‘The Digital Millennium Copyright Act: Preserving the Traditional Copyright Balance’ (2001) 12 *Fordham Intellectual Property, Media and Entertainment Law Journal* 157 at 163; Keller op cit note 21 at 189.

<sup>31</sup> The White Paper op cit note 24 at 231; see also Besek op cit note 20 at 401.

<sup>32</sup> Ibid; Ficsor op cit note 27 para 6.27 at 275; Samuelson op cit note 19 at 411.

provide copyright protection for works not protected by copyright law. The White Paper stresses that technological measures used to protect works not protected by copyright law will not qualify for protection. Where a circumvention device is used in relation to a work in the public domain, such a device will not qualify as a system that ‘prevents or inhibits the violation of any of the exclusive rights of the copyright owner’, as works in the public domain are not protected by copyright law.<sup>33</sup> The Working Group also claims that the primary purpose or effect standard will allow the distribution of devices that deactivate anti-copying devices used in relation to works in the public domain. However, as Kurtz<sup>34</sup> correctly states, it is difficult to imagine a device that can de-activate anti-copying devices only with respect to works in the public domain and leave such devices intact to prevent the copying of copyright works. It would be necessary for those who place unprotected works on the National Information Infrastructure to use a different type of technological protection from that used for copyright works, and the Working Group sees no reason why they should do so. This leaves developers of products with non-infringing uses at the mercy of the uncertain ‘primary purpose or effect’ test.

The White Paper claims that even if its proposal does shield technological protection of works in the public domain, such protection would extend ‘only to those particular copies – not to the underlying works itself’.<sup>35</sup> Vinje<sup>36</sup> criticises this claim:

“This argument assumes that feasible access to public domain materials unencumbered by technical protection will continue to be readily available in the digital world, a questionable assumption. . . . Moreover, it is not clear the basis which the authors of the US White Paper would require a user with lawful access to a work to take the time and incur the expense of obtaining alternative access to the same work in order to make a copy of that work that he is legally entitled to make. . . . Would this not create incentives for firms to buy up the public domain and put it on line, subject to technical protection?”

---

<sup>33</sup> The White Paper op cit note 24 at 231-232; see also Besek op cit note 20 at 401; Ficsor op cit note 27 para 6.27 at 375-376; Kurtz op cit note 3 at 125.

<sup>34</sup> Kurtz op cit note 3 at 125.

<sup>35</sup> The White Paper op cit note 24 at 232. See also Besek op cit note 20 at 402.

<sup>36</sup> Thomas C Vinje ‘A Brave New World of Technical Protection Systems: Will There Still Be Room For

So the concern that works in the public domain could be locked up remained.

The third concern was that the proposals, if adopted, would place an unwarranted burden on manufacturers. The White Paper addresses this concern by underlining that the proposed amendment would not require manufacturers to accommodate any protection systems.<sup>37</sup>

The White Paper accordingly stands by the proposals made in the Green Paper. It suggests the insertion of a new chapter 12 on copyright protection and management systems into the Copyright Act, with the provisions on the ‘circumvention of copyright protection systems’ to be included in a new section 1201. Since the White Paper finds the concerns raised against the proposal in the Green Paper to be unfounded, the text of the draft provision is identical to that in the Green Paper:

‘No person shall import, manufacture or distribute any device, product, or component incorporated into a device or product, or offer or perform any service, the primary purpose or effect of which is to avoid, bypass, remove, deactivate, or otherwise circumvent, without the authority of the copyright owner or the law, any process, treatment, mechanism or system which prevents or inhibits the violation of any of the exclusive rights of the copyright owner under section 106.’

The White Paper does not recommend a prohibition on the act of circumvention. Nor does it explicitly address access or access controls, though to the extent that access controls ‘inhibit’ the violation of exclusive rights they fall within the ambit of this prohibition.<sup>38</sup> However, since access was at this stage not recognized as an exclusive right,<sup>39</sup> it is difficult to imagine which access controls would have ‘inhibited’ the violation of exclusive rights.

---

Copyright?’ [1996] *European Intellectual Property Review* 431 at 437.

<sup>37</sup> The White Paper op cit note 24 at 232; see also Ficsor op cit note 27 para 6.27 at 376.

<sup>38</sup> Besek op cit note 20 at 401.

<sup>39</sup> It is beyond the scope of this chapter to discuss whether users have a ‘right’ to demand access to and the making of non-infringing use of a copyright work. I have throughout this chapter used the words ‘exception’ and ‘limitation’ to connote what is otherwise also referred to as ‘exemptions’ to the exclusive rights held by authors. I will address the question of the access right in Chapter 7.

The White Paper emphasized that its proposal would prohibit only those devices whose primary purpose or effect was to circumvent technological protection measures without authority. Such authority could come from either the author or from the exceptions in the Copyright Act.<sup>40</sup>

The new draft also includes provisions relating to civil remedies (a new section 1203), and criminal offences and penalties (section 1204).<sup>41</sup>

Shortly after the White Paper was issued, two bills incorporating its legislative recommendations were introduced in both houses of Congress.<sup>42</sup> Although hearings were held in the Senate in late 1995 and early 1996, neither bill passed in the 104th Congress.<sup>43</sup>

Meanwhile, the Diplomatic Conference on Certain Copyright and Neighbouring Rights Questions was convened by the World Intellectual Property Organization in Geneva in 1996. The United States made a Proposal for the Protocol to the Berne Convention.

#### **4.2.3 The Proposal for the Protocol to the Berne Convention**

The language of the United States Proposal for the Protocol to the Berne Convention (the 'US Proposal') is nearly identical to the provision contained in White Paper.<sup>44</sup> It contains broad prohibitions, striking not only at circumvention conduct but also circumvention devices.

The only noteworthy difference between the White Paper and the US Proposal is that the Proposal regulates circumvention 'without authority', whereas the White Paper focuses on circumvention 'without the authority of the copyright owner or the law' According to Samuelson,<sup>45</sup> the wording of the US Proposal seems to reflect United States concerns that some countries would circumvent any anti-circumvention regulation that the new instrument

---

<sup>40</sup> The White Paper op cit note 24 at 231; see also Besek op cit note 20 at 401.

<sup>41</sup> The White Paper op cit note 24, appendix 8-12; see also Ficsor op cit note 27 para 6.28 at 376.

<sup>42</sup> S 1284, 104th Cong (1995); HR 2441, 104th Cong (1995).

<sup>43</sup> Besek op cit note 20 at 402.

<sup>44</sup> See also Samuelson op cit note 19 at 373.

might contain by adopting sufficiently broad exceptions so as to enable circumvention to occur ‘with authority of law’.

In the end, though, article 11 of the WCT prohibits only circumvention conduct. However, as I shall show below, when the United States adopted the WCT, it reverted to its original prohibition of conduct and devices, as contained in its proposal.

### **4.3 The Digital Millennium Copyright Act**

#### **4.3.1 Background**

The WCT formed an integral part in the Clinton administration’s ‘Framework for Global Electronic Commerce’. The administration hoped that this treaty would ‘will greatly facilitate the commercial applications of on-line digital communications’.<sup>46</sup>

The implementation of the WCT in national legislation was preceded by intense debate. The question was asked whether the United States actually needed implementing legislation because of the substantial accord between the WCT norms and existing United States law. The Clinton Administration eventually decided that existing law discharged with all its treaty obligations, except those on technological protection measures and rights management information.<sup>47</sup> Even though a number of statutes and judicial decisions had already established anti-circumvention norms,<sup>48</sup> political reality and the legislative dynamics of the WCT implementation process were such that it was believed that some sort of anti-circumvention provision was needed in federal legislation.<sup>49</sup>

The debate about the implementation of the WCT touched on three issues: (a) whether the prohibition should extend to devices as well as to conduct; (b) whether equipment should be required to respond to particular protection measures; and (c) the appropriate exceptions to

---

<sup>45</sup> *Idem* at 411-412.

<sup>46</sup> Susan A Mort ‘The WTO, WIPO & the Internet: Confounding the Borders of Copyright and Neighboring Rights’ (1997) 8 *Fordham Intellectual Property, Media and Entertainment Law Journal* 173 at 210-211.

<sup>47</sup> Jörg Reinbothe & Silke von Lewinski ‘The WIPO Treaties 1996: Ready to Come into Force’ [2002] *European Intellectual Property Review* 199 at 204; Samuelson op cit note 8 at 530-531.

<sup>48</sup> Jeanneret op cit note 30 at 164.

<sup>49</sup> Samuelson op cit note 8 at 532.

the prohibition on circumvention.<sup>50</sup> These three issues reflect the concerns raised against the proposals in the Green Paper. So it is clear that despite the attempts in the White Paper to address them that they remained unresolved.

In July 1997, a bill<sup>51</sup> to implement the WCT was introduced in the House of Representatives by Representative Coble (hence it is also referred to as the ‘Coble Bill’ or the ‘Coble approach’).<sup>52</sup> Its anti-circumvention provisions were more stringent than those in the White Paper and earlier proposals. It proposed the addition of a new chapter 12, entitled ‘Copyright Protection and Management Systems’, to the Copyright Act. The new chapter would prohibit the circumvention of copyright protection systems as well as the destruction of any copyright management information.

The bill contained a specific prohibition on the circumvention of access controls. It prohibited devices to circumvent either access or copy controls. The prohibition extended not only to devices whose ‘primary purpose or effect’ was to circumvent but also to devices marketed for that purpose, or that had no commercially significant purpose or use other than to circumvent.<sup>53</sup>

The White Paper sought to bar only those devices whose primary purpose or effect was to circumvent ‘without the authority of the copyright owner or the law’. This limitation, which would probably have permitted circumvention for non-infringing uses, was not incorporated in the bill. As introduced, the bill contained only one exception – for law enforcement and intelligence activities.<sup>54</sup>

Many objected to the White Paper’s apparent conflict with the ruling of the Supreme Court in *Sony Corporation of America v Universal City Studios Inc*<sup>55</sup> – that manufacturing devices capable of being used for copyright infringement does not, of itself, attract liability for

---

<sup>50</sup> Dean S Marks & Bruce H Turnbull ‘Technical Protection Measures: The Intersection of Technology, Law and Commercial Licences’ [2000] *European Intellectual Property Review* 198 at 2000.

<sup>51</sup> HR 2281, 104th Cong (1997).

<sup>52</sup> *Mort* op cit note 46 at 211.

<sup>53</sup> *Besek* op cit note 20 at 403.

<sup>54</sup> *Ibid.*

<sup>55</sup> *Op cit* note 5. This view was confirmed by the Supreme Court in *Metro-Goldwyn-Mayer Studios Inc v*

copyright infringement.<sup>56</sup>

In 1997, the House Subcommittee on Courts and Intellectual Property of the House Judiciary Committee held hearings on the bill, and it was then referred to the House Committee on Commerce. While the bill was under consideration, another bill<sup>57</sup> (referred to as the ‘Hatch Bill’ or the ‘Hatch approach’),<sup>58</sup> was passed by the Senate on 14 May 1998.

The anti-circumvention provision in the Hatch Bill was largely similar to that in the Coble Bill.<sup>59</sup> However, the Hatch Bill allowed four exceptions to the prohibition on the circumvention of access controls: for law enforcement, for non-profit libraries and archives to examine a work in order to determine whether to acquire it, for reverse engineering to achieve interoperability,<sup>60</sup> and an exception concerning minors and inappropriate material on the Internet.<sup>61</sup>

On 4 August 1998, the House of Representatives passed the Coble Bill. This version of the bill contained some significant modifications to address the concerns about the possible effects of the proposed section 1201 on fair use, and represented a compromise between the House Judiciary Committee and the House Commerce Committee.<sup>62</sup>

As the versions of the WCT implementing legislation passed by the House and Senate differed, a Conference Committee was established. The final version of the Coble Bill was passed by Senate on 8 October 1998, and by the House on 12 October 1998.<sup>63</sup> It was signed by President Clinton and the DMCA became effective on 28 October 1998.<sup>64</sup>

---

*Grokster* 125 S Ct 2764 (2005)).

<sup>56</sup> Mort op cit note 46 at 211-212.

<sup>57</sup> S 2037, 105th Cong (1998).

<sup>58</sup> Mort op cit note 46 at 211.

<sup>59</sup> See Tamber Christian ‘Implementation of the WIPO Copyright Treaty - How Hard Can it Be?’ (1998) 15 *Computer Lawyer* 8 at 10.

<sup>60</sup> Mort op cit note 46 at 212.

<sup>61</sup> Besek op cit note 20 at 404.

<sup>62</sup> Idem at 406.

<sup>63</sup> Idem at 406-407.

<sup>64</sup> Jonathan Band ‘The Digital Millennium Copyright Act: A Balanced Result’ [1999] *European Intellectual Property Review* 92. For a more complete discussion of the legislative progress of the DMCA, see also Besek

The DMCA is designed to ‘facilitate the robust development and world-wide expansion of electronic commerce, communications, research, development, and education in the digital age’.<sup>65</sup> It is divided into five titles that address a number of significant copyright related issues. Only Title I is relevant for present purposes. It amends the Copyright Act to discharge the United States obligations under the WCT.

Title I of the DMCA, then, inserts a new Chapter 12 for into the Copyright Act. This chapter deals with ‘Copyright Protection and Management Systems’. A new section 1201 implements the obligation to provide adequate and effective protection against the circumvention of technological protection measures.

As I stated earlier, three main questions arose during the implementation of article 11 of the WCT: (a) should the prohibition extend to devices as well as conduct? (b) Should equipment be required to respond to particular protection measures? (c) What should be the exceptions to the prohibition on circumvention?<sup>66</sup> The DMCA seeks to answer all three questions.

In the first instance, the anti-circumvention provisions of article 11 of the WCT are silent as to whether they apply to only circumvention conduct, or also to devices and services that are designed or distributed to defeat protection technologies.<sup>67</sup> In its implementation of article 11 in national legislation, the United States decided to prohibit not only the conduct of circumvention but also the trafficking in circumvention devices.<sup>68</sup>

Secondly, whether equipment should be required to respond to certain technologies is addressed by the no-mandate provision.<sup>69</sup>

Thirdly, exceptions to the prohibition on circumvention are specifically included in section 1201.

---

op cit note 20 at 402-407.

<sup>65</sup> ‘Report to Congress: Joint Study of Section 1201(g) of the Digital Millennium Copyright Act’, accessible at <[http://www.loc.gov/copyright/reports/studies/dmca\\_report.html](http://www.loc.gov/copyright/reports/studies/dmca_report.html)>, last visited on 15 February 2007.

<sup>66</sup> Marks & Turnbull op cit note 50 at 200.

<sup>67</sup> Idem at 201.

<sup>68</sup> For a brief account of the hearings on House Bill 2281, during which this issue was discussed, see Christian op cit note 59 at 13-14.

I shall first give a brief exposition of the types of measures that have been treated as technological protection measures, and discuss the prohibitions aimed at the protection of technological protection measures. I shall then refer to the responsibilities placed on equipment manufactures, and the obligations of authors, and the savings provision. Lastly, I shall examine the provisions aimed at limiting the application of section 1201.

### **4.3.2 Technological Protection Measures**

The aim of the prohibition on circumvention is to protect the technological protection measures applied by authors to their works. So it is crucial to determine the meaning of the term ‘technological protection measure’. The Act recognizes two types of technological protection measure – a technological measure ‘that effectively controls *access* to a work’, (access control) and a technological measure ‘that effectively *protects* the right of a copyright owner’ (copy control).

In a number of cases the courts have had the opportunity to determine the meaning of the term ‘technological protection measure’.

In *RealNetworks Inc v Streambox Inc*,<sup>70</sup> the plaintiff had a content delivery system that allowed authors to encode and communicate their works via a ‘Realserver’ to users who could access them using a ‘Realplayer’. The server and player worked together to allow authors to make their works available to users for streaming, but not for copying. Two security mechanisms made this possible: (a) the ‘secret handshake’, an authentication sequence that ensured that content from a ‘Realserver’ was streamed only to a ‘Realplayer’; and (b) a ‘copy switch’ that enabled the author to control the copying of the content. The court regarded the plaintiff’s ‘secret handshake’ and ‘copy switch’ as technological protection measures.

---

<sup>69</sup> 17 USC § 1201(k).

<sup>70</sup> No C99-207OP, 2000 US Dist LEXIS 1889 (WD Wash).

In *Lexmark International v Static Control Components*,<sup>71</sup> the plaintiff used an authentication sequence in its microchips to prevent customers from using cartridges from other manufacturers. The authentication sequence controlled access to the plaintiff's toner and printer programs, which were protected by copyright. The court regarded the authentication sequence as a technological protection measure (an access control).

In *Universal City Studios v Reimerdes*,<sup>72</sup> the defendants operated a website that posted and linked to DeCSS software. DeCSS unlocks the encryption mechanism known as the Content Scramble System (CSS) that protects films on Digital Versatile Discs (DVDs) from being copied or played on non-compliant DVD players or computer drives. The district court concluded that CSS 'effectively control[ed] access' to the films on DVDs, as keys were required to access the films, which keys could not be obtained without a licence or the purchase of an authorized DVD player or drive. The court rejected the defendants' argument that CSS does not control access because it is 'weak' encryption – the statute would be meaningless if it protected only successful technological protection measures.<sup>73</sup> The court also rejected the defendant's arguments that DeCSS was not created to pirate films. That the defendants offered DeCSS on their website was unlawful, regardless of the reason why DeCSS was written.<sup>74</sup>

In *321 Studios v Metro-Goldwyn-Mayer Studios*,<sup>75</sup> the court, like the court in *Reimerdes*, held that CSS was an effective technological measure protection.

*IMS Inquiry Management Systems v Berkshire Information Systems*<sup>76</sup> involved password protection. The court held that password protection on the plaintiff's website qualified as a technological protection measure that effectively controls access to a copyright work. According to the court, entering the password constituted the 'application of information' in order to gain access to the protected work.

---

<sup>71</sup> 253 F Supp 2d 943 (ED Ky 2003).

<sup>72</sup> 111 F Supp 2d 294 (SNDY 2000).

<sup>73</sup> At 317-318.

<sup>74</sup> At 319.

<sup>75</sup> 307 F Supp 2d 1085 (ND Cal 2004).

In *Sony Computer Entertainment America v Gamemasters*,<sup>77</sup> Sony used a technological protection measure that prevented access to the software that operated with Sony's *Playstation* video game console. The console used a technological measure that verified whether a CD-ROM game inserted into the console was an 'authorized, legitimate [Sony] product licensed for distribution in the same geographical territory of the console's sale'. If the console could not verify the game was actually such an authorized product, the console would not operate and the game would not play. The technological measure that prevented access to the software embedded in Sony's *Playstation* console was seen as access control.

In *Lexmark International v Static Control Components*,<sup>78</sup> the defendant argued that the DMCA amendment intended to protect copyright works that have independent market value. The court refused to read such a limitation into section 1201(a)(2) of the Copyright Act. The court held that where a technological protection measure was applied to a protected work, it was protected against circumvention, whether or not the work had independent value. This subparagraph applied to technological measures that protected access 'to a work protected under this title'. In the present case, the computer program in this case was such a work, even though it did not have independent market value. This argument – that the protected work must have an independent market value – would also have failed in the case of section 1201(b), which expressly protects 'a technological measure that effectively protects a right of a copyright owner under this title *in a work or a portion thereof*' (emphasis added). Since even those measures that protect only part of a work are protected, the work to which the measure is applied need not have an independent market value.

In *Pearl Investments LLC v Standard I/O Inc*,<sup>79</sup> the court found that a virtual private network qualified as a technological protection measure – it was the "electronic equivalent" of a locked door'.<sup>80</sup> The court stated that even if no previous court had extended the protection introduced by the DMCA to virtual private networks, that did not mean that the Copyright Act did not protect virtual private networks.

---

<sup>76</sup> 307 F Supp 2d 521 (SDNY 2004).

<sup>77</sup> 87 F Supp 2d 976 (ND Cal 1999)

<sup>78</sup> Supra note 71.

<sup>79</sup> 257 F Supp 2d 326 (D Me 2003) at 350.

<sup>80</sup> Ibid.

These cases offer but a few examples of technology regarded by courts as technological protection measures. However, *Pearl Investments* makes it clear that new and previously unknown protections could also qualify for protection under the Copyright Act.

### 4.3.3 The Prohibition

Section 1201 prohibits the circumvention of technological protection measures, and the trafficking in devices used to circumvent technological protection measures. The section 1201 prohibitions can broadly be divided into two categories: (a) the prohibition on the *conduct* of circumventing access controls (section 1201(a)(1)); and (b) the prohibition on the trafficking in *devices* that circumvent access control (section 1201(a)(2)), or copy control (section 1201(b)).

#### 4.3.3.1 The Prohibition of Conduct

Section 1201(a)(1) contains the prohibition of certain conduct. Section 1201(a)(1)(A) states:

‘No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter.’

Congress delayed the implementation of this prohibition for two years. During this period, the Librarian of Congress, in consultation with the Register of Copyright, had to identify particular classes of works whose users would be ‘adversely affected by the prohibition . . . in their ability to make non-infringing uses under this title of a particular class of copyrighted works’.<sup>81</sup> Section 1201(a)(1) accordingly took effect on 28 October 2000.<sup>82</sup>

The prohibition in section 1201(a)(1)(A) is limited to the circumvention of technological

---

<sup>81</sup> 17 USC § 1201(a)(1)(C).

<sup>82</sup> ‘Report to Congress: Joint Study of Section 1201(g) of the Digital Millennium Copyright Act’ op cit note 65.

measures that prevent unauthorized *access* to a copyright work. There is no similar prohibition on conduct relating to the circumvention of copy controls. According to Ficsor,<sup>83</sup> the reason for this limitation is as follows: in the past, accessing a copyright work was never regarded as an infringement. Only the performance of an act exclusively reserved for an author would be an infringement. Where a protection measure was circumvented merely to gain access to a protected work, the circumvention would not necessarily have led to an infringing act. So it was necessary expressly to prohibit the act of circumventing an access control. Where a protection measure is circumvented in order to perform any of the acts exclusively reserved for the author, such circumvention would lead to infringement. As the circumvention of a copy control would in any event constitute infringement, it is not necessary expressly to prohibit the act of circumventing a copy control.

Section 1201(a)(1)(A) prohibits the act of circumventing an access control even when no infringement results.<sup>84</sup> It accordingly creates a prohibition separate and distinct from copyright infringement. Also, it prohibits *an individual* from circumventing access controls. (It states that “no person” shall circumvent an access control.) Enforcing this prohibition, then, will require instituting action against each individual user. So this prohibition will prove largely impractical to control widespread access and use.<sup>85</sup>

In terms of section 1201(a)(3)(A), the circumvention of a technological measure 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’. Other legislative instruments implementing the WCT, such as the Copyright Directive<sup>86</sup> in Europe, do not contain a specific definition of ‘circumvention’ – it was thought to be sufficiently clear what a proscribed act of circumvention may be. The definition inserted by the DMCA is technology specific and not functional. Ficsor<sup>87</sup> argues that this definition can become obsolete because of the rapid change in technology.

---

<sup>83</sup> Ficsor op cit note 27 at 551 C11.15.

<sup>84</sup> Band op cit note 64 at 92.

<sup>85</sup> Glynn S Lunney Jr ‘The Death of Copyright: Digital Technology, Private Copying, and the Digital Millennium Copyright Act’ (2001) 87 *Virginia Law Review* 813 at 830.

<sup>86</sup> Directive 2001/29/EC of the European Parliament and the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (the Copyright Directive) accessible at <[http://europa.eu.int/documents/comm/index\\_en.htm](http://europa.eu.int/documents/comm/index_en.htm)> (last visited on 11 March 2004)

Section 1201(a)(3)(B) adds that a technological measure must ‘effectively control [...] access to a work’. A measure effectively controls access if it, ‘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’. Ficsor,<sup>87</sup> argues that this subparagraph, read with section 1201(b)(2)(B), offers the correct interpretation of ‘effectiveness’.

In *Realnetworks Inc v Streambox Inc*,<sup>89</sup> Judge Pechman stated that a technological protection measure will be effective if ‘in the ordinary course of its operation [it] restricts and limits the ability of people to make perfect digital copies of a copyrighted work’. According to Judge Kaplan in *Universal City Studios Inc v Reimerdes*,<sup>90</sup> ‘a technological measure ‘effectively controls access’ to a copyrighted work if its *function* is to control access’.

Nimmer,<sup>91</sup> by contrast, states that it is unsure what type of ‘technological measure would effectively control access to a work. To him it seems as if section 1201 attempts to protect measures that did not exist at when the DMCA was passed.

#### **4.3.3.2 The Prohibition on the Trafficking in Circumvention Devices**

Before the enactment of the DMCA, the Copyright Act was technologically neutral. It did not regulate technology or commerce in technology.<sup>92</sup> Despite this traditional technologically neutral approach in the Copyright Act, the United States still decided to implement the WCT prohibition by prohibiting not only *acts* of circumvention but also circumvention *devices*.

There were mainly four arguments raised in favour of the inclusion of a prohibition on devices. In the first instance, it was argued that the regulation of devices was not foreign to United States copyright law – it had a history of suits against technology that allows

---

<sup>87</sup> Ficsor op cit note 27 at 549 C11.11.

<sup>88</sup> Idem at 545.

<sup>89</sup> Supra note 70.

<sup>90</sup> Supra note 72 at 318.

<sup>91</sup> David Nimmer ‘Back From the Future: A Proleptic Review of the Digital Millennium Copyright Act’ (2001) 16 *Berkeley Technology Law Journal* 855 at 860.

<sup>92</sup> David Nimmer ‘A Riff on Fair Use in the Digital Millennium Copyright Act’ (2000) 148 *University of*

copying,<sup>93</sup> and there were already legislative provisions in other areas of law regulate copying devices.<sup>94</sup> Secondly, the prohibition on devices sought to address the concern that the real danger to authors was posed not by individual acts of circumvention but by the manufacture and dissemination of circumvention devices.<sup>95</sup> Thirdly, it was said that a prohibition only of acts of circumvention for infringing purposes added nothing new to existing law, in so far as an author could sue in any event for copyright infringement.<sup>96</sup> Fourthly, as regards the prohibition on the manufacturing, marketing, and dissemination of circumvention devices, it was argued that it would be easier to enforce a prohibition on the trafficking in circumvention devices than what it would be to enforce a prohibition on each individual and private act of circumvention.<sup>97</sup>

Since the courts had already formulated principles to determine the permissibility of devices, the United States legislator had to decide whether these principles discharged the WCT obligation to provide ‘adequate legal protection and effective legal remedies against . . .

---

*Pennsylvania Law Review* 673 at 683.

<sup>93</sup> Some law suits succeeded (such as *Cable/Home Communications Corp v Network Productions Inc* 902 F 2d 829 (11th Cir 1990); *A&M Records Inc v Napster Inc* 239 F 3d 1004 (9th Cir 2001); *Metro-Goldwyn-Mayer Studios Inc v Grokster* op cit note 55); others did not (for example, *Sony Corp v Universal City Studios* op cit note 5.) See also David Nimmer ‘A Tale of Two Treaties Dateline: Geneva - December 1996’ (1997) 22 *Columbia-VLA Journal of Law and the Arts* 1 at 17.

<sup>94</sup> The Audio Home Recording Act (17 USC § 1002(a) and (c)) exercises limited control over technologies as it applies to ‘digital audio recording devices’. The Cable Communications Policy Act (47 USC § 553(a)) states that ‘[n]o person shall intercept or receive or assist in intercepting or receiving any communication service offered over a cable system, unless specifically authorized to do so by a cable operator’. It then defines the phrase ‘[a]ssist in interception or receiving’ to include ‘the manufacture or distribution of equipment intended . . . for unauthorized reception’. Similarly, the satellite decryption provision of the Communications Act (47 USC § 605(e)(3) and (4)) focuses on the manufacture and distribution of a satellite descrambler. Article 1707 (the satellite decryption provision) of the North American Free Trade Agreement (NAFTA) 32 ILM 605 requires that each member country make it ‘a criminal offence to manufacture . . . or otherwise make available a device or system that is primarily of assistance in decoding an encrypted program-carrying satellite signal without the authorization of the lawful distributor of such signal’. Section 2512 of the Electronic Communications Privacy Act (18 USC) prohibits any person from intentionally manufacturing, selling, or possessing any device ‘knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral or electronic communications’.

<sup>95</sup> The Administration’s White Paper stated that ‘technological protection likely will not be effective unless the law also provides some protection for the technological processes and systems used to prevent or restrict unauthorized uses of copyrighted works’ (The White Paper op cit note 24 at 231-232). See Jeanneret op cit note 30 at 164; Vinje op cit note 11 at 198.

<sup>96</sup> According to Vinje (op cit note 11 at 198), it is not so clear that a prohibition on acts of circumvention will add nothing to existing remedies. Where damages are awarded or penalties imposed for circumvention in addition to those available for copyright infringement, the addition of a prohibition could provide a supplemental deterrent to copyright infringement. This would be true especially were additional criminal penalties to be imposed for circumvention, or were circumvention to be taken into account in determining whether copyright infringement should be deemed to be a criminal offence.

circumvention'.<sup>98</sup> If existing principles did not, then the legislator had to formulate new principles.<sup>99</sup>

The vicarious liability standard established by the court in *Sony Corp of America v Universal City Studios*<sup>100</sup> governs the liability of a person who makes available copying technology that enables others to engage in unauthorized copying of a copyright work. Under the *Sony* standard, manufacturing devices capable of being used for copyright infringement is not in itself an infringement.<sup>101</sup> A product is legitimate and may be lawfully manufactured and sold if it is 'capable of a commercially significant non-infringing use'.<sup>102</sup> The fact that the circumvention device is used almost exclusively for purposes of infringement is not sufficient to establish liability: a plaintiff also has to show that the device is incapable of any substantial non-infringing use.

In *Metro-Goldwyn-Mayer Studios Inc v Grokster*,<sup>103</sup> the Supreme Court affirmed the *Sony* standard. However, even if a device were capable of substantial non-infringing use, *intent* to induce infringement would still render the manufacturer or distributor liable for indirect infringement.<sup>104</sup> The court states:

'*Sony's* rule limits imputing culpable intent as a matter of law from the characteristics or uses of a distributed product. But nothing in *Sony* requires courts to ignore evidence of intent if there is such evidence, and the case was never meant to foreclose rules of fault-based liability derived from common law.'<sup>105</sup>

And,

---

<sup>97</sup> Jeanneret op cit note 30 at 179; Lunney op cit note 85 at 830; Vinje op cit note 11 at 198.

<sup>98</sup> Nimmer op cit note 93 at 18-19.

<sup>99</sup> *Idem* at 18.

<sup>100</sup> *Sony Corp v Universal City Studios Inc* op cit note 5.

<sup>101</sup> Mort op cit note 46 at 211-212.

<sup>102</sup> At 442.

<sup>103</sup> *Supra* note 55.

<sup>104</sup> See also Neil A Smith 'Supreme Court Report: Metro-Goldwyn-Mayer Studios Inc et al v Grokster Ltd et al 125 S.Ct. 2764 (2005)' accessible at <<http://www.sheppardmullin.com/images/pubs/pub502.pdf>>, (last visited on 26 June 2006).

<sup>105</sup> At 2779.

‘[t]he question is under what circumstances the distributor of a product capable of both lawful and unlawful use is liable for acts of copyright infringement by third parties using the product. We hold that one who distributes a device *with the object of promoting its use to infringe copyright*, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.’<sup>106</sup>

In discharging the WCT obligation through the DMCA amendments, the United States legislator followed the reasoning that the *Sony* standard was insufficient and that a new test had to be formulated.<sup>107</sup> When one compares sections 1201(a)(2) and 1201(b) to the *Sony* standard, these provisions reduce the degree of involvement required to establish liability, and tie liability to circumvention itself, rather than to a later act of copyright infringement.<sup>108</sup> Under *Sony*, liability turned on the capacity of the device for non-infringing use. By contrast, section 1201 ties liability to the distribution of circumvention devices, even if the resulting access and acts are fair use or otherwise non-infringing.<sup>109</sup> Defendants now face liability also under the Copyright Act and not merely for contributory copyright infringement as in *Sony*.<sup>110</sup> The new prohibitions on devices nullify and replace the *Sony* standard in respect of circumvention devices.<sup>111</sup> The *Sony* standard still applies to devices other than circumvention devices, that are capable of infringing copyright.<sup>112</sup>

---

<sup>106</sup> At 2770 (emphasis added).

<sup>107</sup> Nimmer op cit note 93 at 18.

<sup>108</sup> Lunney op cit note 85 at 832.

<sup>109</sup> Band op cit note 64 at 92; Lunney op cit note 85 at 834-835.

<sup>110</sup> See Denis T Brogan ‘Fair Use no Longer: How the Digital Millennium Copyright Act Bars Fair Use of Digitally Stored Copyrighted Works’ (2002) 16 *St John’s Journal of Legal Commentary* 691 at 723.

<sup>111</sup> Jeanneret op cit note 30 at 171-174. In *Universal City Studios, Inc v Reimerdes* supra 72 at 323, the District Court stated that ‘Sony involved a construction of the Copyright Act that has been overruled by the later enactment of the DMCA to the extent of any inconsistency between Sony and the new statute’. In *Realnetworks v Streambox* supra note 70, the court likewise stressed that section 1201 had superseded the Sony ‘merely capable of non-infringing use’ standard for contributory infringement by manufacturers of devices used to make private copies. Compare the statement by Mary Beth Peters, Register of Copyrights, The On-Line Copyright Liability Limitation Act and the WIPO Copyright Treaties Implementation Act: Hearings on HR 2180 and HR 2281 Before the Subcommittee on Courts and Intellectual Property of the House Committee on the Judiciary, 105th Cong (1997), quoted by Jeanneret op cit note 30 at 182-183. Peters contends that even though the Sony standard by itself is ineffective, the standard built into section 1201 actually builds upon the Sony substantial non-infringing standard.

<sup>112</sup> In *A&M Records Inc v Napster Inc* supra note 93, Napster provided a centralized method for the sharing of files containing protected works, whilst in *Metro-Goldwyn-Mayer Studios Inc v Grokster* op cit note 55, the Grokster and Morpheus software allowed computer users to share copyright works in electronic format through peer-to-peer networks. In both cases the software (or devices used to infringe copyright) was subjected to the

The DMCA established three categories of prohibited services or devices. These categories are alternative, not accumulative.<sup>113</sup> A device, service or component that falls within any of these categories is prohibited and may not be manufactured, imported, sold, or otherwise distributed.<sup>114</sup> The device, service, or component must be applied to a copyright work in order for these provisions of the Copyright Act to apply to such device, service, or component.<sup>115</sup> Also, it is sufficient if only a component or part of a device falls into any of these categories of prohibited services or devices.<sup>116</sup> Where only a part of a device falls into a prohibited category, the whole device is hit by the prohibition.

The first category contains devices that are primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a copyright work.<sup>117</sup> This category appears too clustered around a subjective criterion – did the manufacturer of the device create it for the purposes of circumventing technological protection measures of copyright works? If the manufacturer created it solely for the purpose of circumventing technological protection measures of works not protected by copyright (such as works in the public domain), then this category would not bar the dissemination of such a device.<sup>118</sup>

Where a manufacturer creates a device to circumvent a technological protection measure of a copyright work, the device is prohibited, even if it has non-infringing uses, or if its circumvention does not lead to copyright infringement. The ‘primary purpose’ test in this category is not equivalent to the *Sony* ‘substantial non-infringing use’ test. Therefore, a person would be liable under the DMCA amendments for trafficking in a device primarily

---

Sony standard.

<sup>113</sup> The Act creates three independent bases for liability (*Realnetworks Inc v Streambox Inc* supra note 70; *Lexmark International Inc v Static Control Components Inc* op cit note 71 at 969).

<sup>114</sup> Jane C Ginsberg ‘Copyright Legislation for the “Digital Millennium”’ (1999) 23 *Columbia-VLA Journal of Law and the Arts* 137 at 144; Marks & Turnbull op cit note 50 at 201.

<sup>115</sup> 17 USC § 1201(a)(2) and (b); also *The Chamberlain Group Inc v Skylink Technologies Inc* (ND Ill unreported civil action No 02 C 6376 ) at 23 (affirmed on appeal 381 F 3d 1178 (Fed Cir 2004)).

<sup>116</sup> *321 Studios v Metro Goldwyn Mayer Studios Inc* op cit note 75 at 1098; *Realnetworks Inc v Streambox Inc* supra note 70 at 8; *The Chamberlain Group Inc v Skylink Technologies Inc* supra note 115 at 22-23; see also Marks & Turnbull op cit note 50 at 201.

<sup>117</sup> 17 USC § 1201(a)(2)(A) and 1201(b)(1)(A).

<sup>118</sup> Ginsberg op cit note 114 at 145.

designed to circumvent, even if there is a substantial non-infringing use of the circumvention. This interpretation was followed in *Paramount Pictures Corporation and Twentieth Century Fox Film Corporation v 321 Studios, a/k/a 321 Studios LLC, a/k/a Terr Lcc*,<sup>119</sup> where the court ruled that the ‘primarily’ requirement is not evaded by the existence of arguably limited alternative uses. Also, anyone attempting to help another circumvent a technological measure is liable regardless of whether or not there was a subsequent infringement.<sup>120</sup>

According to Van den Elzen,<sup>121</sup> the DMCA’s radical extension of the *Sony* standard<sup>122</sup> to establish liability could be unconstitutional, because the *Sony* substantial non-infringing use test may be required by the Constitution. The *Sony* court reasoned that the constitutional balance required between economic incentive to create works and public access to works to motivate creativity forbade a ban on a machine that was capable of allowing non-infringing fair use.<sup>123</sup> However, in *321 Studios v Metro Goldwyn Mayer Studios Inc et al*,<sup>124</sup> the court, with reference to *United States v Elcom Ltd*,<sup>125</sup> ruled that the DMCA does not exceed the scope of Congressional powers.

The second category of prohibited devices contains devices that, although not primarily designed to circumvent, actually have ‘only limited commercially significant purpose or use other than to circumvent. . .’<sup>126</sup> It imposes an objective criterion – despite the manufacturer’s intention, how is the device actually being used? If the device has a commercially significant use to access or copy encrypted public domain works, its sale is not prohibited.<sup>127</sup> The phrase ‘has . . . purpose or use’ seems to focus on actual, rather than potential, uses.<sup>128</sup>

---

<sup>119</sup> No 03-CV-8970 RO (SDNY 2004) accessible at <http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/cyberlaw/pp32130304opn.pdf> (visited on 20 March 2007)

<sup>120</sup> Ryan L van den Elzen ‘Decrypting the DMCA: Fair Use as a Defense to the Distribution of DeCSS’ (2002) 77 *The Notre Dame Law Review* 673 at 690.

<sup>121</sup> *Idem* at 696.

<sup>122</sup> Lunney op cit note 85 at 833-834.

<sup>123</sup> At 429 and 442.

<sup>124</sup> *Supra* note 75 at 1103-1105.

<sup>125</sup> 203 F Supp 2d 1111 (ND Cal 2002).

<sup>126</sup> 17 USC § 1201(a)(2)(B) and 1201(b)(1)(B); *Realnetworks Inc v Streambox Inc* *supra* note 70 at 8.

<sup>127</sup> Ginsberg op cit note 114 at 145.

<sup>128</sup> Lunney op cit note 85 at 833-834.

In *The Chamberlain Group Inc v Skylink Technologies Inc*,<sup>129</sup> the court held that a device falling within these first two categories was prohibited even if the device also served another legitimate purpose.

The third category contains circumvention devices ‘marketed’ as such. This prohibition targets the person promoting the circumventing use. She would usually not be the manufacturer, unless the manufacturer acts in concert with the marketer.<sup>130</sup> The full breadth of the ‘is marketed for’ criterion is not clear.<sup>131</sup> However, it appears as if advertising alone would be sufficient to establish liability.<sup>132</sup> It is also irrelevant whether the circumvention device is offered for free over the Internet, or whether it is offered for sale. Both instances are regarded as trafficking in circumvention devices.<sup>133</sup> In *321 Studios v Metro Goldwyn Mayer Studios Inc et al*,<sup>134</sup> the plaintiff claimed that this prohibition against marketing violated the First Amendment that protects freedom of expression. The court stated that ‘the First Amendment does not protect commercial speech that involves illegal activity. . .’<sup>135</sup>

The prohibition on devices has three consequences.

In the first instance, it creates a new form of liability for third parties. A person can be found liable absent a direct copyright infringement on someone’s part. Unlike contributory infringement and vicarious liability, which both require infringement to establish third party liability, the anti-trafficking provisions can impose liability on a person for providing the means to circumvent a technological protection measure, even where it enables lawful use.<sup>136</sup>

Secondly, by prohibiting the devices necessary to circumvent technological protection measures for non-infringing purposes, the prohibition makes it impossible to perform non-infringing acts. So despite the list of exceptions stated in section 1201, the adoption of the

---

<sup>129</sup> Op cit note 115 at 22.

<sup>130</sup> 17 USC 1201(a)(2)(C) and 1201(b)(1)(C); see also Ginsberg op cit note 114 at 144.

<sup>131</sup> Ginsberg op cit note 114 at 145.

<sup>132</sup> Lunney op cit note 85 at 837.

<sup>133</sup> *Paramount Pictures Corporation and Twentieth Century Fox Film Corporation v 321 Studios a/k/a 321 Studios LLC a/k/a Terr Lcc* supra note 119.

<sup>134</sup> Supra note 75.

<sup>135</sup> At 1098.

<sup>136</sup> Van den Elzen op cit note 120 at 691-692.

broad device prohibition would in many instances render these exceptions meaningless.

Thirdly, Band and Isshiki<sup>137</sup> question whether an online service provider that hosts a site that makes circumvention devices available is liable for ‘trafficking’ in those devices, even if it had no knowledge of the presence of the devices on the site. Although such service provider would probably not face criminal liability if it had no knowledge, it might well incur civil liability.

In contrast to the prohibition on the act of circumvention, which applies only to the circumvention of access control, the prohibition on devices also relates to copy control.

#### **4.3.3.2.1 The Manufacture and Distribution of Devices that Circumvent Access Controls**

Section 1201(a)(2) contains a technology related prohibition: it prohibits the making or distribution of a device used to circumvent a technological measure that prevents access to a copyright work. This provision does not target those who access a protected work without authorization but rather those who facilitate the process of accessing a protected work.<sup>138</sup>

It is usually easy to identify circumvention devices used to circumvent access controls, such as encryption.<sup>139</sup> Although the protection introduced by the DMCA is not limited to encryption, I shall briefly examine this measure as it is presently the most common type of

---

<sup>137</sup> Jonathan Band & Taro Isshiki ‘The New US Anti-Circumvention Provision: Heading in the Wrong Direction’ (1999) 15 *Computer Law & Security Report* 219 at 224-225.

<sup>138</sup> Op cit note 92 at 687.

<sup>139</sup> In *Realnetworks Inc v Streambox Inc* supra note 70, the plaintiff’s ‘secret handshake’ was regarded as a type of access control governed by section 1201(a)(2). In *Sony Computer Entertainment America v Gamemasters* supra note 77 at 981, Sony had used a technological measure that prevented access to the protected computer software that operated with Sony’s Playstation video game console. The console used a technological measure that verified whether a CD-ROM game inserted into the console was an ‘authorized, legitimate [Sony] product licensed for distribution in the same geographical territory of the console’s sale’. If the console could not verify that the game actually was such an authorized product, the console did not operate and the game did not play. The technological measure that prevented access to software embedded in Sony’s Playstation console was treated as an access control, and the device that circumvented this measure was found to be a circumvention device, even though it did not facilitate piracy (at 987). In *Lexmark International Inc v Static Control Components Inc* supra note 71 at 968-969, the authentication sequence in the plaintiff’s microchips, which controlled access to the plaintiff’s protected toner and printer programs, was treated as an access control. In *Pearl Investments LLC v Standard I/O Inc* supra note 79 at 350, the court held that a virtual private network

access control. A device can either pass encrypted content along without descrambling it, or the device can descramble the content to make it viewable or accessible by the end user.

Where the device passes the encrypted content unaltered, it does not circumvent the access control. But where the device descrambles the content, an access control is circumvented. A device cannot descramble encrypted content by accident. Decryption requires affirmative action by the device to ‘unlock’ the controls on the content and so to make it accessible.<sup>140</sup>

Section 1201(a)(2) applies to devices used to circumvent technological protection measures that provide access to a work ‘protected under this title’ – copyright works. So this provision applies to devices used to circumvent access controls on copyright works. The problem with this prohibition is that where a person wants to access a protected work for non-infringing purposes, she still may not circumvent any access control, as that would violate this provision. I shall address this problem in more detail in my discussion of ‘fair use’ below.

Again, only those technological measures that ‘effectively controls access to a work’ are protected. A measure effectively controls access if it requires the application of a measure, with the authority of the author, to gain access to the work in question.<sup>141</sup> In *321 Studios v Metro Goldwyn Mayer Studios Inc et al*,<sup>142</sup> the plaintiff questioned whether the technological protection measure (CSS, in this case) was an effective control or protection of DVDs, as the CSS access keys were widely available on the Internet. The court held:

‘However, this is equivalent to a claim that, since it is easy to find skeleton keys on the black market, a deadbolt is not an effective lock. Moreover, the statute itself defines “effectively protects a right of a copyright owner under this title” to mean “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.”<sup>143</sup>

---

qualified as a technological protection measure as it was the ““electronic equivalent” of a locked door”.

<sup>140</sup> Marks & Turnbull op cit note 50 at 201.

<sup>141</sup> 17 USC § 1201(a)(3)(B).

<sup>142</sup> Supra note 75.

<sup>143</sup> At 1095.

The court then referred to the following passage in *Universal City Studios Inc v Reimerdes*:<sup>144</sup>

‘One cannot lawfully gain access to the keys except by entering into a licence with the DVD CCA under authority granted by the authors or by purchasing a DVD player or drive containing keys pursuant to such a licence. In consequence, under the express terms of the statute, CSS ‘effectively controls access’ to copyrighted DVD movies. *It does so, within the meaning of the statute, whether or not it is a strong means of protection.*’

In *Pearl Investments LLC v Standard I/O Inc*,<sup>145</sup> the court agreed - whether a technological measure ‘effectively controls access’ was analysed solely with reference to how the measure worked ‘in the ordinary course of its operation’. The court added that the mere fact that a defendant had alternative means to access the copyright works was irrelevant to the question as to whether the technological protection measure effectively controlled access to the work in question.<sup>146</sup>

The same objections raised against the prohibition on the conduct of circumventing an access control can be raised against the prohibition of devices used to circumvent access control.

#### **4.3.3.2.2 The Prohibition on the Manufacture and Distribution of Devices that Circumvent Copy Controls**

Section 1201 does not prohibit the act of circumventing copy control. Although the initial proposed wording of section 1201(b) contained such a prohibition,<sup>147</sup> the Clinton Administration eliminated this provision in response to the concerns of the library and education communities about the negative impact of such legislation on fair use. The Administration suggested that by eliminating the prohibition on the circumvention of copy control, a library engaged in such circumvention for purposes of archival copying<sup>148</sup> will not

---

<sup>144</sup> Supra note 72 at 317-318 (emphasis added).

<sup>145</sup> Supra note 79.

<sup>146</sup> At 350.

<sup>147</sup> Similar to the prohibition in 17 USC § 1201(a)(1).

<sup>148</sup> Permitted under 17 USC § 108.

incur liability.<sup>149</sup> This was also stated in *United States v Elcom Ltd.*<sup>150</sup>

‘Congress did not ban the act of circumventing the use restrictions. Instead, Congress banned only the trafficking in and marketing of devices primarily designed to circumvent the use restriction protective technologies. Congress did not prohibit the act of circumvention because it sought to preserve the fair use rights of persons who had lawfully acquired a work.’

Section 1201(b) prohibits the manufacturing and distribution of any technology used for the circumvention of measures that protect ‘a right of a copyright owner under this title in a work or a portion thereof’. (It is sometimes referred to as the ‘additional violations’ provision.<sup>151</sup>) Like section 1201(a)(2), section 1201(b) contains a technology related prohibition.

Section 1201(b) applies to devices used to circumvent technological protection measures that protect an author’s exclusive rights of authorization (‘a right of a copyright owner under this title’). So this provision expressly applies to protection measures that prevent copyright infringing acts. As only those technological measures that prevent infringement are protected, it should theoretically be possible to engage in circumvention for non-infringing purposes.

However, despite the belief that non-infringing uses will be permitted because the conduct of circumventing copy control is not expressly prohibited, and because only technological protection measures that prevent infringing acts are protected against circumvention, the practical result of section 1201(b) is that circumvention for non-infringing use is inhibited. As this provision prohibits the manufacture of devices that could circumvent copy control, users do not have the technological tools with which to engage in the circumvention necessary for non-infringing use.<sup>152</sup>

Also, section 1201(b) is aimed not at those who actually infringes copyright, but at rather at

---

<sup>149</sup> Jeanneret op cit note 30 at 167; Vinje op cit note 11 at 202.

<sup>150</sup> Supra note 125 at 1120.

<sup>151</sup> Jeanneret op cit note 30 at 166.

<sup>152</sup> Band & Isshiki op cit note 137 at 220; Jeanneret op cit note 30 at 167; Vinje op cit note 11 at 202. Cf Ginsberg op cit note 114 at 152-153: she argues that if a device is manufactured for fair use, and is used for this

those who facilitates copyright infringement.<sup>153</sup> It prohibits not the use of circumvention devices but the ‘manufacture, import, offer to the public, provide, or otherwise traffic’ in these devices. Why is the use itself is not prohibited? The answer is that a prohibition on use would target individual infringers, which would make enforcement largely impractical.

Devices that circumvent copy control are less easy to identify than those used to circumvent access control, because the successful operation of copy control technology usually depends on a response from the playback or recording device. With encryption (a type of access control), if the playback device does not affirmatively respond to unlock the content, the content remains encrypted and protected. With copy control flags, by contrast, if the device does not affirmatively look for and respond to the flags, then the content is not protected and open to unauthorized copying. It is not so much that computers override or remove this type of protection but rather computers do not ‘look for’ and respond to them.<sup>154</sup> So the question arises as to whether a device that fails to respond to a copy control should be regarded as a circumvention device for the purposes of this prohibition.

Another interesting point was made in *321 Studios v Metro Goldwyn Mayer Studios Inc.*<sup>155</sup> There the court held that if a work was copied without circumventing the access control, the copying would ‘not be particularly useful’, as any copy made without circumventing such control could not be accessed or viewed.<sup>156</sup> In order to make a useful copy, not only the copy control but also the access control had to be circumvented. Often one device would perform both these two functions simultaneously, and so it could happen that the same device would be prohibited under both section 1201(a)(2) and section 1201(b)(1).

#### **4.3.4 The Responsibility of Equipment Manufacturers**

The consumer electronics and computer industries were concerned about the possibility that video cassette recorders (VCRs) and personal computers (PCs) might have to respond to

---

purpose, there is no violation of section 1201(b).

<sup>153</sup> Nimmer op cit note 91 at 689-691.

<sup>154</sup> Marks & Turnbull op cit note 50 at 201-202.

<sup>155</sup> Supra note 75.

<sup>156</sup> At 1097.

copy protection technology.<sup>157</sup> They also feared that they might be required to retrofit VCRs and PCs already on the market to accommodate new forms of protection that may be incorporated in protected material in future.<sup>158</sup>

Authors, for their part, believed that equipment manufacturers should not be permitted to design their products purposely so as to avoid copy protection technology. This issue was resolved by the DMCA enactment of what is known as the ‘no mandate’ provision. Section 1201(c)(3) clarifies that the prohibition on circumvention devices does not require devices to respond affirmatively to any particular technological measure, as long as the device does not otherwise fall within one of the three prohibited categories of devices.<sup>159</sup>

However, despite this general ‘no mandate’ rule, section 1201(k) does place a responsibility on the manufacturers of analogue VCRs – within eighteen months of the enactment of the DMCA, all analogue VCRs had to be designed to conform to the two forms of copy control technology that widely used in the market today – automatic gain control technology, and ‘colour stripe’ copy control technology. This provision prohibits tampering with these analogue copy control technologies to render them ineffective by the redesigning of VCRs, or by the intervention of ‘black box’ devices or ‘software hacks’.<sup>160</sup>

Ginsberg<sup>161</sup> explains the reason for an informed response for this category of works:

‘This chapter offers a welcome, if belated and incomplete, response to the supreme Courts decision in *Sony Corp. of America v. Universal City Studios, Inc.*, in which a majority of the Court rejected liability for contributory infringement of the manufacturers and distributors of videocassette recorders, on ground that the recorders were capable for a non-infringing fair use, in that case, time shifting of free

---

<sup>157</sup> Copy control, generally, depends on a positive response from the playback or recording device (Marks & Turnbull op cit note 50 at 202.)

<sup>158</sup> Vinje op cit note 11 at 204.

<sup>159</sup> Marks & Turnbull op cit note 50 at 202. In *Realnetworks Inc v Streambox Inc* supra note 70, the defendant invoked section 1201(c)(3) to resist the finding of a section 1201(b) violation. However, the court emphasized that section 1201(c)(3) applies only ‘so long as such part or component, or the product in which such part or component is integrated, does not otherwise fall within the prohibitions of §§ (a)(2) or (b)(1)’.

<sup>160</sup> Vinje op cit note 11 at 204.

<sup>161</sup> Ginsberg op cit note 114 at 155-156.

broadcast television programming. The Court never held that *retaining* copies of recorded programs, or recording pay-TV or cable programming was fair use, but in practice, the public engaged in all these varieties of uncompensated taping, and copyright owners initiated no further suits. Unlike many European countries, the U.S. never instituted a levy on the media or equipment of videocassette recorders in order to compensate copyright owners, authors and performers of audiovisual works. Section 1201(k) now addresses the problem of home videotaping by prohibiting the manufacture and distribution of certain analog videocassette recorders unless the recorders are equipped with a designated copy control technology.<sup>162</sup>

The copy control technology works in tandem with audiovisual works and transmissions that have been encoded to prevent or limit consumer copying. Section 1201(k), however, restricts the instances in which an author or some other person may encode the audiovisual work or transmission: transmissions of live events; transmissions of audiovisual works delivered on a pay-per-view basis; copies of transmissions of live events or of audiovisual works made available through a subscription to a television channel; a physical medium containing one or more pre-recorded audiovisual works; and copies of transmissions of live events or of pay-per-view motion picture transmissions, or copies made from a physical medium containing pre-recorded audiovisual works.<sup>163</sup> So a person may not encode television broadcasts that can be accessed without payment. Consumers may continue to time shift (or even retain) copies of ‘free’ television programmes.<sup>164</sup>

Although it is not part of section 1201, a new Federal Communications Commission ruling places an additional responsibility on equipment manufacturers: digital television sets manufactured on or after 1 July 2005 are required to implement a technological protection measure for digital broadcast television, which measure is known as the ‘broadcast flag’.<sup>165</sup> It allows content owners to insert a data signal in the broadcast stream that will cause receivers to respond to restrict the copying and redistribution of digital broadcast programs by

---

<sup>162</sup> Congress did, by contrast, institute a blank tape and equipment levy in respect of digital audio recording devices (17 USC §§ 1001-1010).

<sup>163</sup> 17 USC § 1201(k)(2).

<sup>164</sup> Ginsberg op cit note 114 at 156.

<sup>165</sup> *In re Digital Broadcast Content Protection, Report and Order and Further Notice of Proposed Rulemaking*,

consumers.

### 4.3.5 The Obligations of Authors

The Copyright Act allows transmitting organizations to make ‘ephemeral’ copies of sound recordings for purposes of transmission or archival preservation.<sup>166</sup> Authors are required to make available to a transmitting organization ‘the necessary means for permitting the making of such phonorecord as permitted under this subsection, if it is technologically feasible and economically reasonable for the copyright owner to do so’.<sup>167</sup> If the author fails to meet this requirement in a timely manner, ‘the transmitting organization shall not be liable for a violation of § 1201(a)(1) of this title for engaging in such activities as are necessary to make such phonorecords as permitted under this section’.<sup>168</sup>

Apart from these provisions, there is no statutory duty on an author to provide a beneficiary of a copyright exception with the means to take advantage of such exception.<sup>169</sup> However, if a user is unable to take advantage of a statutory privilege, the Librarian of Congress may create an exception to the prohibition on the circumvention of access controls.<sup>170</sup> This may affect not only an author’s choice of technological protection measures but also her decision whether or not to continue to market the work without technological protection.<sup>171</sup>

### 4.3.6 Limiting the Application of Section 1201

As originally proposed, section 1201 had no limits on its application. Concerns arose that such broad legislation would create a technological monopoly over all uses of copyright

---

MB Docket 02-230, FCC 03-273 (4 November 2003), cited by Besek op cit note 20 at 425.

<sup>166</sup> 17 USC § 112(e).

<sup>167</sup> 17 USC § 112(e)(8).

<sup>168</sup> Besek op cit note 20 at 398-399.

<sup>169</sup> In this important respect the Copyright Act differs from the Copyright Directive in Europe: article 6.4 of the Directive requires Member States to take appropriate measures to ensure that users have the means to benefit from certain specified exemptions or limitations in the law, provided that the beneficiary has legal access to the protected works. It also allows (but does not require) Member States, absent voluntary measures by authors, to take ‘appropriate measures’ in order to enable users to take advantage of ‘private use’ exemptions in national laws. On-demand services are exempt from this requirement. See Besek op cit note 20 at 393.

<sup>170</sup> 17 USC § 1201(a)(1)(B)-(E).

<sup>171</sup> Besek op cit note 20 at 398.

works, and that it would inhibit not only infringing use but also many non-infringing uses. Accordingly, as the Bill advanced through Congress, numerous exceptions were crafted onto section 1201.<sup>172</sup>

The DMCA attempted to avoid the pitfalls of over broad copyright protection in two ways. In the first instance, the Act contained three provisions that called for further studies on the legal protection of technological protection measures. Secondly, the Act introduced a savings provision, and stated specific and detailed exceptions to the circumvention prohibitions.<sup>173</sup>

As I shall show below, it does not seem as if these attempts to limit the application of section 1201 will actually succeed in doing so. And even if they do, Band,<sup>174</sup> for one, fears that the patchwork of prohibitions and exceptions will encourage litigation and impede innovation.

I shall first explore the ongoing monitoring processes, then the savings clauses, and lastly the specific exceptions.

#### **4.3.6.1 Ongoing Monitoring**

The DMCA provided for three monitoring processes – the rule-making process of the Librarian of Congress, a study concerning encryption research and technology, and a study under section 104 of the DMCA.

##### **4.3.6.1.1 Rule-making by the Librarian of Congress**

The prohibition on circumventing access control is subject to an exemption for users of a work that falls into a particular class of works if the prohibition adversely affects, or is likely adversely to affect, their non-infringing uses.<sup>175</sup> The Librarian of Congress must determine the applicability of this exemption during a periodic rule-making – after the initial two-year

---

<sup>172</sup> Vinje op cit note 11 at 202.

<sup>173</sup> Michael Hart ‘The Copyright in the Information Society Directive: An Overview’ [2002] *European Intellectual Property Review* 58 at 62.

<sup>174</sup> Band & Isshiki op cit note 137 at 220.

<sup>175</sup> 17 USC § 1201(a)(1)(B).

period, the Librarian of Congress must make such determination during each three-year period after the initial two year period.<sup>176</sup> She must do so on recommendation of the Register of Copyrights, who has to consult with the Assistant Secretary of Commerce for Communications and Information.<sup>177</sup>

Even though the prohibition on acts of circumvention were suspended for two years pending the rule-making, the prohibition on the manufacture and distribution of devices that circumvent access and copy control took immediate effect. So the Librarian of Congress may create only further exemptions from section 1201(a)(1) (the prohibition on the circumvention of access control). The determinations of the Librarian will, therefore, not affect potential liability under the anti-trafficking provisions.

Proponents of an exemption shoulder the burden of proof to show by a preponderance of evidence that there has been, or is likely to be, a substantial adverse effect on non-infringing uses by users of copyright works. De minimis problems, isolated harm, or mere inconvenience are insufficient to carry this burden. A proponent must prove on a preponderance of evidence that the harm is more likely than not; she may not rely on mere speculation. Also, a causal link between the circumvention prohibition and the alleged harm must be shown.<sup>178</sup>

Only ‘classes of works’ may be exempted from the prohibition. Deciding on a particular class of works must be based on the attributes of the works themselves, and not by reference to some external criteria such as the intended use or users of such works. The starting point for any definition of a particular class of works is the categories of works in section 102 of the Copyright Act. But these categories are only a starting point – a ‘class’ for the purposes of this exception will usually be some sub-category of a section 102 category. The determination of the scope of a class of works also considers the likely adverse effects on non-infringing uses and the adverse effects an exemption may have on the market for or

---

<sup>176</sup> 17 USC § 1201(a)(1)(C) and (D).

<sup>177</sup> 17 USC § 1201(a)(1)(C).

<sup>178</sup> Federal Register: 31 October 2003, vol 68 no 241, pp 62011-62018 at 62012, accessible at <<http://www.copyright.gov/fedreg/2003/68fr2011.pdf>> (last visited on 28 February 2007).

value of copyright works.<sup>179</sup>

A particular class of works should further be refined by reference to other factors that assist in ensuring that the scope of the class addresses the scope of the harm to non-infringing uses. A class may, for example, in part be defined with reference to the medium on which the works are distributed. But classifying a work solely by reference to the medium on which the work appears, or the access control measure applied to the work, would be beyond the scope of what a particular class of work is intended to be. It is also not permissible to classify the work by reference to the type of user or intended use.<sup>180</sup>

The following factors should guide the inquiry:<sup>181</sup> (i) the availability for use of copyright works; (ii) the availability for use of works for non-profit, archival, preservation, and educational purposes; (iii) the impact of the prohibition on the circumvention of technological measures applied to copyright works; (iv) the effect of the circumvention of technological measures on the market for or value of copyright works; and (v) such other factors as the Librarian considers appropriate.

#### **4.3.6.1.1.1 The Initial Rule-Making Proceeding**

During the initial two-year period the first section 1201 rule-making proceeding took place. The Librarian of Congress issued its determinations on 27 October 2000. The Librarian exempted only two classes of works.

The first exemption was for ‘compilations consisting of lists of web sites blocked by filtering software applications’, which were used to prevent minors’ access to pornography. Such software was used by schools, libraries, and parents to prevent minors from accessing pornography. This class included copyright compilations of encrypted lists of web sites to which the software denied access. If these lists were used to criticize these sites, such use would have been fair and thus non-infringing. But to learn which web sites were included in

---

<sup>179</sup> Ibid.

<sup>180</sup> Ibid.

<sup>181</sup> 17 USC § 1201(a)(1)(C).

these lists, the lists would have had to be decrypted. In the absence of this exemption, such decryption would have violated section 1201(a)(1).<sup>182</sup>

The second exemption was for literary works, including computer programs and databases, protected by access control measures that failed to allow access because of malfunction, damage, or obsolescence.<sup>183</sup> On general principles, where an access control failed to allow a user lawful access, she could not access the work and was not allowed to circumvent the failed access control to make non-infringing use of the work. Such a result would not have served the interests of authors that section 1201(a)(1) sought to protect. Moreover, the Registrar found that potential damage to authors from this exemption would be minimal – in most cases where it applied they already had been compensated for access to the work.<sup>184</sup>

These two exemptions expired on 27 October 2003. The next day, the Librarian of Congress issued four new exemptions.<sup>185</sup>

#### **4.3.6.1.1.2 The Second Rule-Making Proceeding**

The following four classes of works are exempted from the prohibition on circumvention for from 28 October 2003 until 27 October 2006.<sup>186</sup>

The first exemption was for '[c]ompilations consisting of lists of Internet locations blocked by commercially marketed filtering software applications that are intended to prevent access to domains, web sites or portions of web sites, but not including lists of Internet locations blocked by software applications that operate exclusively to protect against damage to a computer or computer network or lists of Internet locations blocked by software applications that operate exclusively to prevent receipt of e-mail'.<sup>187</sup> For purposes of this exemption,

---

<sup>182</sup> David Goldberg & Robert J Bernstein 'The Prohibition on Circumvention and the Attack on the DVD' [2001] *European Intellectual Property Review* 160 at 163.

<sup>183</sup> Reinbothe & Lewinski op cit note 47 at 205; Charlotte Waelde 'The Quest for Access in the Digital Era: Copyright and the Internet' 2001 (1) *The Journal of Information, Law and Technology (JILT)* at 8, accessible at <<http://elj.warwick.ac.uk/jilt/01-1/waelde.html>>.

<sup>184</sup> Goldberg & Bernstein op cit note 182 at 163.

<sup>185</sup> Federal Register: 31 October 2003 op cit note 178 at 62013.

<sup>186</sup> Ibid.

<sup>187</sup> 'U.S. Copyright Office – Statement of the Librarian of Congress Relating to Section 1201 Rulemaking',

‘Internet locations’ were defined to include ‘domains, uniform resource locators (URLs), numeric IP addresses or any combination thereof.’<sup>188</sup> The class of works consisted of lists of blocked Web sites that were used in various filtering software programs<sup>189</sup> intended to prevent access to domains, web sites, or parts of web sites. The purpose of these programs was to prevent children and other Internet users from viewing objectionable material while online.

Although this exemption was similar to one of the exemptions in the previous rule-making, proponents had to argue their case afresh. While providers of filtering software offered some information about the web sites that their software blocked, such information was too limited to permit comprehensive or meaningful analysis. Those who wanted to review, comment on, and criticize such software as part of an ongoing debate on a matter of public interest had to be permitted to gain access to the complete list of blocked web sites. This exempted class specifically excluded lists of Internet locations blocked by software designed to protect against damage to computers (such as firewalls and anti-virus software), or software designed to prevent receipt of unwanted e-mail (such as anti-spam software).<sup>190</sup>

The second exemption concerned ‘[c]omputer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete’.<sup>191</sup> This class was also similar to a class exempted in 2000, but again the class exempted in 2003 was rather more limited. It was limited to computer programs using ‘dongles’ (hardware locks) that controlled access to the programs. When a dongle was damaged or malfunctioned in such a way that the authorized user of the software could not gain access to the software, she had to be given a means to make the software work. This exempted class included only software that actually could not be accessed due to a damaged or a malfunctioning dongle, and only when the dongle could not be replaced or repaired. It was also required that the dongle be ‘obsolete’ – ‘if [it] is no longer manufactured or is no longer reasonably available in the commercial

---

accessible at <[http://www.copyright.gov/1201/docs/librarian\\_statement\\_01.html](http://www.copyright.gov/1201/docs/librarian_statement_01.html)>, last visited on 2 March 2004.

<sup>188</sup> Federal Register: 31 October 2003 op cit note 178 at 62013.

<sup>189</sup> Sometimes referred to as ‘censorware’.

<sup>190</sup> Federal Register: 31 October 2003 op cit note 178 at 62013.

<sup>191</sup> ‘U.S. Copyright Office – Statement of the Librarian of Congress Relating to Section 1201 Rulemaking’, op cit note 187.

marketplace’.<sup>192</sup> This exemption allowed users who were denied access as a result of a damaged or malfunctioning dongle to circumvent the technological protection measure when repair or replacement was not an option.<sup>193</sup>

The Copyright Office clarified that this exemption applied only to dongles that actually malfunctioned, and not to those that might have malfunctioned at some later stage. As long as the dongle continued to provide access to the work, this exemption did not apply.<sup>194</sup>

The third exemption related to ‘[c]omputer programs and video games distributed in formats that have become obsolete and which require the original media as a condition of access’.<sup>195</sup> This was a new exemption. The Register stated that to the extent that libraries and archives wanted to make preservation copies of published software and video games that were distributed in formats that were obsolete, such activity was a non-infringing use covered by the Copyright Act.<sup>196</sup> So the exempted class was limited to works distributed in now-obsolete formats. Again, “obsolete” has the same meaning that is set forth in section 108(c): a format was considered to be obsolete if the machine or system necessary to render perceptible a work stored in that format was no longer manufactured or reasonably available in the commercial marketplace. This class was also limited to computer programs and video games, as the evidence on record did not support a broader class of works.<sup>197</sup>

The Copyright Office again stated that this exemption applied only to those formats that had already become obsolete. The systematic conversion of works to modern storage formats did not fall within the privilege of section 117 of the Copyright Act to make archival copies in case of software malfunction, nor was it likely to be deemed fair use.<sup>198</sup>

The fourth exemption concerned ‘[l]iterary works distributed in ebook format when all existing ebook editions of the work (including digital text editions made available by

---

<sup>192</sup> 17 USC § 108(c).

<sup>193</sup> Federal Register: 31 October 2003 op cit note 178 at 62013.

<sup>194</sup> Besek op cit note 20 at 421.

<sup>195</sup> ‘U.S. Copyright Office – Statement of the Librarian of Congress Relating to Section 1201 Rulemaking’, op cit note 187.

<sup>196</sup> 17 USC § 108(c).

<sup>197</sup> Federal Register: 31 October 2003 op cit note 178 at 62014.

authorized entities) contain access controls that prevent the enabling of the ebook's read-aloud function and that prevent the enabling of screen readers to render the text into a "specialized format".<sup>199</sup> This exemption was based upon proposals by the American Foundation for the Blind and five major library associations, and was a response to problems experienced by the blind and visually impaired in gaining meaningful access to literary works distributed as e-books. By using digital rights management tools that implicate access controls, publishers of e-books can disable the read-aloud function of an e-book and may prevent access to a work in e-book form by means of screen reader software. Screen reader software is a separate program for the blind and visually impaired that interacts with an e-book reader and is capable of converting the text into either synthesized speech or braille. The disabling of these two functions was alleged to prevent the blind and the visually impaired from engaging in particular non-infringing uses (such as private performance), and, generally, from accessing these works. The uses that such persons make by using the 'read aloud' function and screen readers are not infringing, and are likely to be the most reasonable means of meaningful access for such persons to works that are published in e-book format. To be included in this exempted class, a literary work had to exist in e-book format. This exemption was not available if any existing edition of the work permitted the 'read aloud' function or was screen reader enabled.<sup>200</sup>

These exemptions expired on 27 October 2006. With effect from 27 November 2006, the Librarian of Congress issued six new exemptions.

#### **4.3.6.1.1.3 The Third Rule-Making Proceeding**

From 27 November 2006 to 27 October 2009, the prohibition against circumventing access control does not apply to people who engage in non-infringing uses of the following six exempted classes of works.

The first class of works are '[a]udiovisual works included in the educational library of a

---

<sup>198</sup> Besek op cit note 20 at 422.

<sup>199</sup> 'U.S. Copyright Office – Statement of the Librarian of Congress Relating to Section 1201 Rulemaking', op cit note 187.

<sup>200</sup> Federal Register: 31 October 2003 op cit note 178 at 62014.

college or university's film or media studies department, when circumvention is accomplished for the purpose of making compilations of portions of those works for educational use in the classroom by media studies or film professors'.<sup>201</sup>

A number of film and media professors argued that, in order to teach their classes effectively, they need to be able to create compilations of portions of films for purposes of classroom performance. These films are distributed on DVDs protected by CSS. The professors argued that in order to show the educationally necessary, high-quality content in a reasonably efficient manner, they must circumvent CSS in order to extract the portions necessary for their educational use.<sup>202</sup>

The proponents of this exemption demonstrated that the reproduction and public performance of portions of films or other audiovisual works in the course of face-to-face teaching of film and media studies would, generally, amount to non-infringing use. There were also no alternative means to meet their needs. They demonstrated that the DVD versions of motion pictures often are of higher quality than copies available in other formats, and contain attributes that are, for various reasons, extremely important to teaching about films. One such reason is that the DVD version of a film can preserve the original colour of older films, something that other available formats cannot do.<sup>203</sup>

Authors were concerned that an exemption for a 'class of works' would necessarily exempt a much broader range of uses than those in which the film professors wished to engage. A class of works must be based primarily on the attributes of the work itself, and not the nature of the use or the user. So by recognizing this class not only the film professors, but also others engaging in entirely different uses, would benefit. Authors also believed that this exemption would create confusion about the circumstances in which circumvention was appropriate.<sup>204</sup>

The Registrar concluded that these concerns of authors could be addressed without denying

---

<sup>201</sup> Federal Register: 27 November 2006, vol 71 no 227, pp 68472-68480 at 68473-68474, accessible at <<http://www.copyright.gov/1201>>, (visited on 20 February 2007).

<sup>202</sup> *Idem* at 68474.

<sup>203</sup> *Ibid.*

<sup>204</sup> *Ibid.*

an exemption that will enable the film professors to engage in the non-infringing uses that they have identified. The Registrar concluded that, given the appropriate factual showing, it is permissible to refine the definition of a ‘class’ of works by reference to particular types of user, and/or use.<sup>205</sup>

This class is refined by reference to both the user and the use, as follows: ‘when circumvention is accomplished for the purpose of making compilations of portions of those works *for educational use* in the classroom by *media studies or film professors*’<sup>206</sup> (emphasis added).

The second class of works contains ‘[c]omputer programs and video games distributed in formats that have become obsolete and that require the original media or hardware as a condition of access, when circumvention is accomplished for the purpose of preservation or archival reproduction of published digital works by a library or archive. A format shall be considered obsolete if the machine or system necessary to render perceptible a work stored in that format is no longer manufactured or is no longer reasonably available in the commercial marketplace’.<sup>207</sup>

The Internet Archive proposed this exemption, which is identical to the class of works exempted in the 2003 rule-making proceeding. There was no direct opposition to this request, apart from a concern by authors that many old video games and computer programs are being reintroduced into the market in new ways by their authors, who wished to exclude from the exemption video games that have been re-released on a new gaming platform, because circumvention of access controls would cause significant harm to authors in their exploitation of these re-released works.<sup>208</sup>

Because preservation and archival use is the sole basis for this exemption sought by the Internet Archive, and because the Registrar has determined that in appropriate cases, the definition of a class of works may be refined by reference to particular users and/or uses, the

---

<sup>205</sup> Ibid.

<sup>206</sup> Ibid.

<sup>207</sup> Ibid.

<sup>208</sup> Ibid.

concerns of authors can be addressed by such a refinement. The Internet Archive has established that its archival and preservation activities are non-infringing and that computer programs and video games distributed in formats that have become obsolete and require the original media or hardware as a condition of access constitute works protected by access control. Without the ability to circumvent such access control, the Internet Archive could not engage in its preservation and archival activities with respect to these works.<sup>209</sup>

The third class of works includes ‘[c]omputer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete. A dongle shall be considered obsolete if it is no longer manufactured or if a replacement or repair is no longer reasonably available in the commercial marketplace.’<sup>210</sup>

A number of commentators proposed this renewal of an existing exemption from 2003, which, in turn, was a modified version of one of the exemptions from the 2000 rule-making. In both previous rule-makings, evidence was presented that damaged or malfunctioning dongles can prevent authorized access to the protected software. The legal and analytical rationale for this exemption remains unchanged. The Registrar concluded that a sufficient factual showing was made to support the renewing of this exemption for another three years. The description of this class was refined to include a description of what constitutes an ‘obsolete’ dongle.<sup>211</sup>

In the fourth class of works are ‘[l]iterary works distributed in e-book format when all existing e-book editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling either of the book’s read-aloud function or of screen readers that render the text into a specialized format’.<sup>212</sup>

The American Foundation for the Blind advocated this proposed renewal of an existing exemption for e-books for which the ‘screen readers’ and the ‘read-aloud’ function have been disabled. These functions enable the blind to ‘read’ the text of an e-book by rendering the

---

<sup>209</sup> Idem at 68474-68475.

<sup>210</sup> Idem at 68475.

<sup>211</sup> Ibid.

<sup>212</sup> Ibid.

written text of the book into audible, synthetic speech. Screen readers also allow the text and layout of a text screen to be conveyed spatially so that a blind user can perceive the organization of a page on a screen, or even the organization of a work as a whole and navigate through that book.<sup>213</sup>

Some literary works are distributed in e-book form with the read-aloud and screen reader functions disabled through the use of digital rights management tools. A user would have to circumvent access control in order to alter the usage settings of such e-books in order to enable read-aloud and screen reader functionality.<sup>214</sup>

The previous exemption for this class of works applied only if there was no e-book edition of the work that contained access controls that enabled *both* the e-book's read-aloud function *and* screen readers. The exemption was modified so that it now applies to a literary work when all existing e-book editions of the work contain access controls that prevent the enabling *either* of the book's read-aloud function *or* of screen readers that render the text into specialized format.<sup>215</sup>

The fifth exemption is for '[c]omputer programs in the form of firmware that enable wireless telephone handsets to connect to a wireless telephone communication network, when circumvention is accomplished for the sole purpose of lawfully connecting to a wireless telephone communication network'.<sup>216</sup>

The Wireless Alliance and Robert Inkerton proposed an exemption for 'computer programs that operate wireless communications handsets'. The proponents of this exemption stated that providers of mobile telephony (cellular phone) networks are using various types of software locks in order to control customer access to the 'bootloader' programs on cellular phones and the operating systems programs embedded inside these phones. This software locks prevent customers from using their handsets on a competitor's network by controlling access to the

---

<sup>213</sup> Ibid.

<sup>214</sup> Ibid.

<sup>215</sup> Idem at 68475-68476.

<sup>216</sup> Idem at 68476.

software that operates the cellular phones.<sup>217</sup>

The Registrar concluded that the software locks are access controls that adversely affect the ability of consumers to make non-infringing use of the software on their cellular phones. The four factors listed in section 1201(a)(1)(C)(i)-(iv) of the Copyright Act support the conclusion that an exemption is warranted.<sup>218</sup>

The authors who did express concern about the proposed exemption hold copyright in music, sound recordings, and audiovisual works; their works are offered for downloading onto cellular phones. They expressed concern that the proposed exemption might permit the circumvention of access controls that protect their works when they have been downloaded onto cellular phones. The proponents of the exemption provided assurances that there was no intention that the exemption be used to permit unauthorized access to those works. The exemption was sought for the sole purpose of permitting owners of cellular phone handsets to switch their handsets to a different network.<sup>219</sup>

As the Registrar had concluded that, in appropriate circumstances, a class of works may be refined by reference to the uses made of the works, this issue could best be resolved by modifying the proposed class of works to extend only to ‘computer programs in the form of firmware that enable wireless telephone handsets to connect to a wireless telephone communication network, when circumvention is accomplished for the sole purpose of lawfully connecting to a wireless telephone communication network’.<sup>220</sup>

In the sixth exempted class of works are ‘[s]ound recordings, and audiovisual works associated with those sound recording, distributed in compact disc format and protected by technological protection measures that control access to lawfully purchased works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing,

---

<sup>217</sup> Ibid.

<sup>218</sup> Ibid.

<sup>219</sup> Ibid.

<sup>220</sup> Ibid.

investigating, or correcting such security flaws or vulnerabilities’.<sup>221</sup>

The proposal for this exemption was based on the facts arising out of the distribution of compact discs that used certain digital rights management software that created security vulnerabilities on computers on which the software was installed. SunnComm’s *MediaMax* content protection software and First4Internet’s *XCP* copy protection software programs were specifically identified.<sup>222</sup>

The evidence demonstrated that *MediaMax* and *XCP* controlled access to the sound recordings on a number of compact discs distributed in 2005 and that these access controls created security vulnerabilities on the personal computers on which they were installed.<sup>223</sup>

Authors opposed this proposed exemption primarily on the ground that they believed that there already was a statutory exemption that permitted circumvention of access controls ‘for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network’.<sup>224</sup> But whilst it appears that this exemption may permit circumvention in cases such as those involving *MediaMax* and *XCP*, it is not clear whether this was the case. So in view of this uncertainty and the seriousness of the problem, this last exemption was recommended and accepted.<sup>225</sup>

#### **4.3.6.1.4 Evaluation**

It seems uncertain whether the rule-making authority of the Librarian of Congress will provide a safe haven for non-infringing uses.

My first concern is theoretical. The fact ‘that only classes of works’ may be exempted from the circumvention prohibition, and not the intended use of the copyright work, is not in line

---

<sup>221</sup> *Idem* at 68477.

<sup>222</sup> *Ibid.*

<sup>223</sup> *Ibid.*

<sup>224</sup> 17 USC §1201(j).

<sup>225</sup> Federal Register: 27 November 2006 op cit note 201 at 68477.

with general copyright principles. Exceptions under copyright law are usually made with reference to use (such as ‘fair use’), and not with reference to a specific class of works. Again it seems as if the DMCA amendments ignored traditional copyright law, and not necessarily on good cause having been shown.

Secondly, unlike most other copyright disputes, whether a person is likely to suffer an adverse effect is not made by a court called upon to adjudicate the matter. Instead, the Copyright Office engages in rule making.<sup>226</sup>

Thirdly, the scope of the rule-making differs from that of most of the regulations promulgated by the Copyright Office or the Librarian of Congress. Whereas most regulations administer only technical aspects of copyright law, the present rule making take the additional step of exempting entire categories of potential defendants from liability.<sup>227</sup>

Fourthly, the determinations of the Librarian of Congress cannot be asserted as a defense to an anti-device claim.<sup>228</sup> Although users are entitled, after the Librarian’s determination, to ‘hack’ technological protection systems for any classes of works the non-infringing uses of which have been inhibited, the legislation does not allow the manufacture or distribution of the devices necessary to perform such acts of circumvention. It appears that the Librarian’s determinations would make such user self-help available only if a user can perform the act without a device.<sup>229</sup> Also, as Samuelson<sup>230</sup> correctly remarks, the Librarian has the authority only to assess the ban on the act of circumvention. But considering the act of circumvention without considering the ban on circumvention devices is to ignore the technology regulating provisions in the DMCA amendments. The prohibition on devices can harm competition and innovation in the information technology industry as much as the ban on the act of circumvention can harm non-infringing use. According to Samuelson, the Librarian should also be entitled to consider the impact of anti-device rules on the ability to make non-infringing use of copyright works.

---

<sup>226</sup> Nimmer op cit note 91 at 696.

<sup>227</sup> Idem at 697-698.

<sup>228</sup> 17 USC § 1201(a)(1)(E).

<sup>229</sup> Samuelson op cit note 8 at 560; Vinje op cit note 11 at 204.

<sup>230</sup> Samuelson op cit note 8 at 561.

Fifthly, Band,<sup>231</sup> Cohen,<sup>232</sup> and Nimmer<sup>233</sup> raise the possibility that rule-making provision may violate the separation of powers mandated by the Constitution.<sup>234</sup> The Library of Congress is part of Congress and thus it may not have the constitutional authority to issue regulations. Although the Copyright Office can issue regulations, section 1201(1)(c) provides that the Copyright Office merely makes a recommendation to the Librarian of Congress, who then issues the rule. It remains to be seen whether this constitutional flaw can be separated from the rest of section 1201, or whether it poisons the entire section. Cohen<sup>235</sup> believes that this rule-making procedure cannot be severed from the circumvention ban, and that if this procedure violates the separation of powers, it is likely that the circumvention ban will also fail.

The main objection that Nimmer<sup>236</sup> levels at the rule-making process is that it requires the Librarian of Congress and the Register of Copyrights to predict the future. He cites the complaint of the Copyright Office that ‘the Commerce Committee Report does not state how future adverse impacts are to be evaluated’.<sup>237</sup> The Office also quoted a leading proponent of exemptions as admitting that ‘the inquiry into whether users of works protected by copyright are likely to be adversely affected by the full implementation of section 1201(a)(1) is necessarily “speculative since it entails a prediction about the future”’.<sup>238</sup>

---

<sup>231</sup> Band & Isshiki op cit note 137 at 223.

<sup>232</sup> Julie E Cohen ‘WIPO Copyright Treaty Implementation in the United States: Will Fair Use Survive?’ [1999] *European Intellectual Property Review* 236 at 238.

<sup>233</sup> Nimmer op cit note 91 at 871-873.

<sup>234</sup> Under the Constitution, legislative branch actions must satisfy the requirements of bi-cameralism (consideration by both Houses of Congress) and presentment (submission to the President for signature or veto). Congress may delegate specific grants of rule-making authority to agencies of the executive branch only as long as these grants are consistent with the constitutional authority of that branch to enforce the laws. Congress may not vest rule-making or enforcement authority in an official if it has the power to direct or control that official’s actions, or remove her from office. Although the Librarian of Congress is appointed by the President, the Library of Congress and the Copyright Office are part of the legislative branch, subject to the supervision of Congress. When President Clinton signed the Bill into law, he issued a statement that the Copyright Office is, ‘for constitutional purposes’, part of the executive branch, and that he would accordingly not interpret the Bill as authorizing Congress to exert direct control over the DMCA’s oversight process. But the President cannot relocate the Copyright Office (and, by implication, the Library of Congress) within the executive branch simply by issuing a statement (see Cohen op cit note 232 at 238).

<sup>235</sup> Cohen op cit note 232 at 238.

<sup>236</sup> Nimmer op cit note 91 at 870.

<sup>237</sup> Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed Reg 64555 (27 October 2000) at 64559, cited by Nimmer op cit note 91 at 870.

<sup>238</sup> Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control

Sixthly, exemptions made by the Librarian of Congress may differ from three-year period to three-year period. This can contribute to uncertainty, especially among lay people, men, as to whether or not a particular class of works is actually exempted.

#### **4.3.6.1.2 Study Concerning Encryption Research and Technology**

The Register of Copyrights and the Assistant Secretary for Communications and Information of the Department of Commerce were required to report jointly to Congress, one year after the DMCA came into force, on the effects of section 1201 on encryption research and encryption measures.<sup>239</sup> The report concluded that, at the time, there was no discernable impact on encryption research or encryption technology, and that any legislative recommendations in connection with section 1201(*g*) would be premature.<sup>240</sup>

#### **4.3.6.2 The Savings Clauses**

Section 1201 contains two general savings clauses: section 1201(*c*)(1) provides that nothing in section 1201 affects rights, remedies, limitations, or defences to copyright infringement; and section 1201(*c*)(2), that nothing in section 1201 enlarges or diminishes vicarious or contributory copyright infringement.

##### **4.3.6.2.1 Section 1201(*c*)(1) and the Fair Use Doctrine**

Section 1201(*c*)(1) refers expressly to the fair use doctrine. At first blush, it seems as if this provision recognizes that defences to copyright infringement, and especially fair use, can also be used to defeat actions for the circumvention of technological protection measures.

However, after the enactment of the DMCA, a protracted debate ensued as to whether fair use would indeed be a valid defence to an action for a violation of section 1201.

---

Technologies, 65 Fed Reg 64555 (27 October 2000) at 64562-64563 (quoting Peter Jaszi), cited by Nimmer op cit note 91 at 870.

<sup>239</sup> 17 USC § 1201(*g*)(5),

<sup>240</sup> US Copyright Office, Joint Study of Section 1201(*g*) of the Digital Millennium Copyright Act, accessible at <[http://www.copyright.gov/reports/studies/dmca\\_report.html](http://www.copyright.gov/reports/studies/dmca_report.html)>, cited by Besek op cit note 20 at 423.

Before I discuss the implications of this savings clause, a few brief remarks about the fair use doctrine. The doctrine is codified in section 107 of the Copyright Act. It offers a general and flexible defence to copyright infringement that can be granted by the courts on a case-to-case basis.<sup>241</sup> In line with the common-law origins of the doctrine of fair use, the Act does not provide a definitive list of uses that are fair. Rather, it states four factors that a court has to consider in order to determine whether a particular use is fair: (a) the purpose and character of the use, including whether such use is commercial or for non-profit educational purposes; (b) the nature of the copyright work; (c) the amount and substantiality of the portion used in relation to the copyright work as a whole; and (d) the effect of the use upon the potential market for or value of the copyright work.

According to the proponents of the DMCA, the savings clause under discussion preserves all the traditional defenses available under copyright law, including fair use. Under Ginsberg's syntax theory,<sup>242</sup> this provision permits reading a fair use limitation into the DMCA. Section 1201 covers only technological protection measures applied to copyright works, and so circumvention remains copyright dependant. The same defences available to claims of copyright infringement would then be available to claims for circumvention.<sup>243</sup> Ginsberg states:

'Section 1201 is under Title 17, even if it is not, technically, a provision addressed to copyright infringement. If fair use is a general limitation on rights set out in Title 17, including, for example, the (technically) extra-copyright right to fix performances of musical works set out in section 1101, then section 1201(c) preserves fair use as to anti-circumvention as well.'<sup>244</sup>

---

<sup>241</sup> Séverine Dusollier 'Exceptions and Technological Measures in the European Copyright Directive of 2001 - An Empty Promise' (2003) 34 *ICC* 62 at 64.

<sup>242</sup> Jane C Ginsberg 'From Having Copies to Experiencing Works: the Development of an Access Right in U.S. Copyright Law', accessible at <[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=222493](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=222493)>, cited by Pete Singer 'Mounting a Fair Use Defense to the Anti-Circumvention Provisions of the Digital Millennium Copyright Act' (2002) 28 *University of Dayton Law Review* 111 at 127.

<sup>243</sup> Ginsberg op cit note 114 at 151-152.

<sup>244</sup> Jane C Ginsberg 'Copyright Use and Excuse on the Internet' (2000) 24 *Columbia-VLA Journal of Law & The Arts* 1 at 8-9; see also Tricia J Sadd 'Fair Use as a Defense under the Digital Millennium Copyright Act's Anti-Circumvention Provisions' (2001) 10 *George Mason Law Review* 321 at 343.

She also argues that since fair use is a ‘general equitable defence’, Congress did not intend to limit the development of fair use to rights formally within the Copyright Act. The courts may, in appropriate circumstances, apply fair use to section 1201(a) by articulating additional limitations on the circumvention prohibition.<sup>245</sup> Elsewhere she states that ‘[p]erhaps, under appropriate circumstances, the act of accessing should be deemed fair use as well’.<sup>246</sup>

It has been argued that fair use is preserved not only by section 1201(c)(1), but also by the distinction made in section 1201(a) and (b). The Copyright Office clearly states that the distinction between the prohibition of access and the prohibition of infringement was specifically adopted to preserve fair use.<sup>247</sup> Fair use applies only to lawful access. Since access has always been a precondition of fair use, the anti-circumvention provisions do not truly constitute a change in the manner in which fair use is invoked.<sup>248</sup>

Proponents of section 1201 also argue that the copyright balance has not shifted, as ‘it has long been accepted in U.S. law that the copyright owner has the right to control access to his work, and may choose not to make it available to others or to do so only on set terms’.<sup>249</sup> The anti-circumvention provisions merely continue this tradition. One cannot circumvent a technological protection measure without authorization in order to make fair use of a digital work.<sup>250</sup>

Lastly, it has been argued that Congress intended fair use still to apply in future contexts. This is evident from the legislative history of the codification of fair use. Congress did not intend to freeze the doctrine of fair use in a rigid timeframe. Rather, it expected the courts to continue evolving fair use principles in the course of common-law adjudications, ‘especially

---

<sup>245</sup> Ginsberg op cit note 244 at 9.

<sup>246</sup> See Ginsberg op cit note 114 at 151-152.

<sup>247</sup> ‘The Digital Millennium Copyright Act of 1998: U.S. Copyright Office Summary’, accessible at <<http://www.loc.gov/copyright/legislation/dmca.pdf>> (visited on 18 March 2002)

<sup>248</sup> The On-Line Copyright Liability Limitation Act and the WIPO Copyright Treaties Implementation Act: Hearings on H.R. 2180 and H.R. 2281 before the Subcommittee on Courts and Intellectual Property of the House Committee on the Judiciary, 105th Congress (1997) (statement of Mary Beth Peters, Register of Copyrights), cited by Jeanneret op cit note 30 at 181.

<sup>249</sup> Ibid.

<sup>250</sup> Idem at 182.

during a period of rapid technological change'.<sup>251</sup>

According to the critics of the DMCA, section 1201 does not allow a fair use defense.<sup>252</sup> Various reasons are given. The anti-circumvention provision in section 1201 constitutes a violation separate and distinct from copyright infringement.<sup>253</sup> Liability under section 1201(c)(1) and (2) arises not for copyright infringement but for violation of section 1201.<sup>254</sup> A violation of section 1201 is unlawful regardless of whether it results in infringement.<sup>255</sup> And the DMCA introduces its own civil and criminal remedies, over and above the remedies available for copyright infringement.

Since section 1201 creates a liability separate and distinct from that for copyright infringement, the same defenses available against a claim for copyright infringement would not be available against a claim based on a violation of section 1201. This was recognized during a Congressional hearing on the DMCA, where some representatives of major copyright industries expressed the view that fair use (or other copyright exceptions) should not be an acceptable reason to 'break' a technological protection measure. Allan Adler,<sup>256</sup> testifying on behalf of the Association of American Publishers, gave the following example:

'[T]he fair use doctrine has never given anyone a right to break other laws for the stated purpose of exercising the fair use privilege. Fair use doesn't allow you to break into a locked library in order to make "fair use" copies of books in it, or steal newspapers from a vending machine in order to copy articles and share them with a friend.'

So the savings clause under discussion does accordingly not allow a violator of section 1201 to rely on the same defenses available against copyright infringement. Section 1201(c)(1)

---

<sup>251</sup> Singer op cit note 242 at 122.

<sup>252</sup> See, generally, Brogan op cit note 110.

<sup>253</sup> Singer op cit note 242 at 128.

<sup>254</sup> Lunney op cit note 85 at 839.

<sup>255</sup> Jeanneret op cit note 30 at 168-169.

<sup>256</sup> WIPO Copyright Implementation Act; and Online Copyright Liability Limitation Act: Hearing on H.R. 2281 and H.R. 2280 before the Subcommittee on Courts and Intellectual Property of the House Committee on the Judiciary, 105th Congress (1997) at 208 (prepared statement of Allan Adler), cited by Samuelson op cit note 8 at 539.

merely states that no existing rights, remedies, limitations, and so on are affected.<sup>257</sup> This was confirmed in *Universal City Studios Inc v Reimerdes*,<sup>258</sup> where the court noted that the fair use defence was not available, as there was no claim of copyright infringement in the section 1201 action. The court stated that ‘[i]f Congress had meant the fair use defence to apply to such actions, it would have said so’.<sup>259</sup> Several writers<sup>260</sup> support the *Reimerdes* arguments. So fair use, the traditional defence to a claim of copyright infringement, does not apply to circumvention.<sup>261</sup>

Even if it is accepted that the savings clause does allow for a fair use defence against a claim for circumvention, it might effectively be nullified by section 1201(b)(1), which outlaws technologies necessary to accomplish circumvention.<sup>262</sup> Section 1201 does not contain any provision enabling the development or distribution of circumvention devices to enable fair use. According to Brogan,<sup>263</sup> ‘. . . it is the implicit ban on anti-circumvention measures that spells the shrinking of the fair use doctrine as applied to digital media’. The District Court in *Reimerdes*<sup>264</sup> thought the same: ‘. . . Congress elected to leave technologically unsophisticated persons who wish to make fair use of encrypted copyrighted works without the technological means of doing so. . .’

Critics of the DMCA attack the argument that the fact that Congress did not prohibit the conduct of circumventing copy controls preserves fair use.<sup>265</sup> Once again Congress failed to appreciate that as long as section 1201 prohibits the manufacture of devices that can

---

<sup>257</sup> Compare Sadd op cit note 244 at 343.

<sup>258</sup> 82 F Supp 2d 211 (SDNY 2000).

<sup>259</sup> At 219.

<sup>260</sup> Band & Isshiki op cit note 137 at 219; Jeanneret op cit note 30 at 168; Lunney op cit note 85 at 839-40; Jason Sheets ‘Copyright Misused: The Impact of the DMCA Anti-circumvention Measures on Fair & Innovative Markets’ (2000) 23 *Hastings Communications and Entertainment Law Journal* 1 at 16; Vinje op cit note 11 at 202.

<sup>261</sup> In *Universal City Studios Inc v Reimerdes* op cit note 258 at 219, the court held that Congress did not fold fair use into the DMCA. See also Goldberg & Bernstein op cit note 182 at 162; Jeanneret op cit note 30 at 168.

<sup>262</sup> National Research Council *The Digital Dilemma: Intellectual Property in the Information Age* 2000 National Academy Press at 175; Samuelson op cit note 8 at 555 and 564.

<sup>263</sup> Brogan op cit note 110 at 724.

<sup>264</sup> *Supra* note 72 at 324. In *Universal City Studios Inc v Reimerdes* *supra* note 258 (ordering preliminary injunction), *Universal City Studios Inc v Reimerdes* *supra* note 72 (ordering permanent injunction), and *Universal City Studios Inc v Corley* 273 F 3d 429 (2nd Cir 2001) (affirming permanent injunction), three different courts found, on the same facts, that the defendants’ DeCCS software violated the anti-circumvention provisions of the Copyright Act.

<sup>265</sup> Goldberg & Bernstein op cit note 182 at 160.

circumvent copy control, fair users have no way of engaging in the circumvention necessary to exercise their privilege. An author can fence in her work with technological protection and so prevent purchasers from making fair use copies, by virtue of the unavailability of the necessary circumvention devices.<sup>266</sup>

Also, the mere fact that section 1201 expressly provides for a separate set of exceptions seems to confirm that fair use and other traditional exceptions do not apply to the circumvention prohibition.

Although the Librarian of Congress may exempt classes of works, it is unsure whether this rule-making will address the fair use concerns. Three questions arise. In the first instance, is it constitutional for an administrative body, as opposed to the legislature and the judiciary, to regulate the copyright balance? Secondly, should an exemption system not rather be based on the use to which a work is put than on ‘classes of works’?<sup>267</sup> Thirdly, even if it is accepted that the rule-making process is constitutional, what kind of fair use exemptions will it yield? For procedural and substantive reasons, the exemptions, if any, that emerge from the process are likely to be both narrower than and different from the ‘rules’ of fair use that have previously been developed by the courts. The Copyright Act also expressly provides that an exception established by the Librarian of Congress may not be used as a defence in an action to enforce any other provision introduced by the DMCA.<sup>268</sup> It is unlikely that this rule-making process will address traditional fair use concerns.

Despite the arguments that section 1201 will not disturb fair use, it seems likely that it will at least narrow the scope of the doctrine.<sup>269</sup> Nimmer<sup>270</sup> summarizes the position: ‘The upshot is

---

<sup>266</sup> Band & Isshiki op cit note 137 at 220; Jaqueline Lipton ‘Copyright in the Digital Age: A Comparative Survey’ (2001) 27 *Rutgers Computer and Technology Law Journal* 333 at 356. Compare Ginsberg op cit note 114 at 152-153, who argues that if a device is manufactured for a fair use, and used for fair use purposes, there is no violation of section 1201(b) of the Copyright Act.

<sup>267</sup> Vanessa van Coppenhagen ‘Copyright and the WIPO Copyright Treaty, with Specific Reference to the Rights Applicable in a Digital Environment and the Protection of Technological Measures’ (2002) 119 *South African Law Journal* 429 at 448.

<sup>268</sup> 17 USC § 1201(a)(1)(E).

<sup>269</sup> In *Universal City Studios Inc v Reimerdes* supra note 72 at 346, the court stated that the defendants ‘have raised a legitimate concern about the possible impact on traditional fair use of access control measures in the digital era’.

<sup>270</sup> Nimmer op cit note 91 at 716.

that fair use would apply only following lawful access, not as a basis for obtaining such access in the first instance.’

In several cases the argument was raised that the elimination of fair use could render section 1201 unconstitutional.

In *Universal City Studios Inc v Corley*,<sup>271</sup> the appellants argued that fair use is constitutionally protected, and that the DMCA as applied by the District Court in *Reimerdes*<sup>272</sup> eliminates fair use. The Supreme Court states that it ‘. . . has never held that fair use is constitutionally required. . .’. Although the court refers to several decisions, in the end it decides that it need not explore the extent to which fair use may have constitutional protection, as this is beyond the scope of the suit before the court.

In *Realnetworks Inc v Streambox Inc*,<sup>273</sup> the court likewise rejected the defendant’s fair use argument.

And in *United States v Elcom Ltd*,<sup>274</sup> and *321 Studios v Metro Goldwyn Mayer Studios Inc*<sup>275</sup> it was held that the DMCA did not impermissibly violate users’ fair use privileges.

Violators of the circumvention prohibition, then, do not have a general fair use defence at their disposal but will have to rely on the specific and narrow exemptions and exceptions stated in section 1201.

#### **4.3.6.2.2 Section 1201(c)(2)**

Section 1201(c)(2) states that nothing in section 1201 enlarges or diminishes liability for

---

<sup>271</sup> Supra note 264 at 458.

<sup>272</sup> Supra note 72.

<sup>273</sup> Supra note 70.

<sup>274</sup> Supra note 125. Here, the defendant was criminally prosecuted for violations of the anti-circumvention prohibition. The defendant developed and sold a product, the Advanced eBook Processor, which allowed a user to remove the use restrictions from electronic books and allowed the book easily to be reproduced and distributed electronically. The defendant filed a motion to dismiss the indictment, based on the unconstitutionality of the DMCA. After the motion was denied, the defendant was tried and acquitted by a jury.

<sup>275</sup> Supra note 75 at 1101-1103.

vicarious or contributory copyright infringement in connection with any technology, product, service, device, component, or part of it. This provision implies that a person using or dealing with a circumvention device will be liable for contributory copyright infringement under the principles established in *Sony*,<sup>276</sup> and for a contravention of the anti-circumvention provisions of section 1201. As I explained earlier, the standard to determine the admissibility of a device used in *Sony* is different from that established under section 1201. So the same set of facts can establish two kinds of liability, and the circumvention device in question will be tested by two different standards.

#### **4.3.6.3 Exceptions to Authorize Legitimate Circumvention**

Congress enacted new statutory exceptions in section 1201 to authorize legitimate circumvention. Unlike the principles of fair use, these exceptions are precise and narrowly drawn.

I shall briefly examine each exception. Some of them apply to the basic prohibition on the act of circumvention, others to this prohibition and that on trafficking, and others to all three circumvention prohibitions.<sup>277</sup>

##### **4.3.6.3.1 Non-profit Libraries, Archives, and Educational Institutions**

The prohibition on the act of circumventing an access control is subject to an exception that permits non-profit libraries, archives, and educational institutions to circumvent a technological protection measure solely for the purpose of making a good faith determination as to whether they wish to obtain authorized access to the work.<sup>278</sup> A qualifying institution may gain access only when it cannot obtain a copy of an identical work by other means, and access may not last longer than necessary. This means that the institutions listed may defeat the access code, for example, only in order to make a purchasing decision, and not for any other purpose. Such an entity may not use this exception for commercial advantage or

---

<sup>276</sup> *Sony Corp v Universal City Studios Inc* supra note 5.

<sup>277</sup> According to Nimmer op cit note 91 at 701-702, no reason can be found in the statute itself or its legislative history to justify this differentiation.

financial gain. The library and educational associations did not request this exception. Rather, it was gifted to them by the House Subcommittee on Courts and Intellectual Property, so that the subcommittee could claim that it responded to the concerns of libraries and schools.<sup>279</sup>

Special protection of non-profit libraries, archives, and educational institutions is provided not only by this exception but also by section 1203. These institutions are entitled to a complete remission of damages in civil actions,<sup>280</sup> and are entirely exempted from criminal liability.<sup>281</sup> But the person who enables them to circumvent a technological protection measure (by offering circumvention services, or by providing circumvention devices) is not exempted. In practice, this may create a situation in which these institutions do not have the necessary means to engage in circumvention.

Vinje<sup>282</sup> believes that this exception is of little practical use, not only because of the unavailability of the means to circumvent, but also because it is unlikely that a content provider will refuse access to a potential customer, particularly large institutional customers such as libraries and schools.

#### **4.3.6.3.2 Law Enforcement and Intelligence Activities**

The Copyright Act allows circumvention, and the development of circumvention devices, for any lawfully authorized investigative, protective, or intelligence activity by a federal, state, or local government employee, or a person under contract to federal, state, or local government.<sup>283</sup> It also allows the private sector to develop circumvention devices for use by the government in law enforcement.

#### **4.3.6.3.3 Reverse Engineering**

One of the most vital copyright exceptions is the one relating to software interoperability.

---

<sup>278</sup> 17 USC § 1201(d).

<sup>279</sup> Vinje op cit note 11 at 204.

<sup>280</sup> 17 USC § 1203(c)(5)(B).

<sup>281</sup> 17 USC § 1204(b).

<sup>282</sup> Vinje op cit note 11 at 204.

(‘Interoperability’ is ‘the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged’.<sup>284</sup>) To achieve interoperability, computer software and hardware developers must have access to their competitors’ interface specifications. The reverse engineering process technically requires ‘reproductions’ and ‘translations’ to be made of the software being analysed. So copyright law, generally, permits the reproduction and translation inherent in software reverse engineering.<sup>285</sup>

The reverse engineering exception to the prohibition on circumvention was introduced by the Hatch Bill, which expressly exempted reverse engineering ‘necessary to achieve interoperability of an independently created computer program with other programs’, provided that (a) the necessary elements of such computer program were not otherwise readily available, and (b) the study and analysis of the computer programming did not constitute copyright infringement.<sup>286</sup>

According to the report of the Senate Judiciary Committee, this exception was ‘intended to allow legitimate software developers to continue engaging in certain activities for the purpose of achieving interoperability to the extent permitted by law prior to the enactment of this chapter’.<sup>287</sup> The Committee cited *Sega Enterprises Ltd v Accolade Inc*,<sup>288</sup> and stated that ‘[t]he objective is to ensure that the effect of current case law interpreting the Copyright Act is not changed by enactment of this legislation for certain acts of identification and analysis done in respect of computer programs’, and that ‘[t]he purpose of this action is to foster competition and innovation in the computer and software industry’.<sup>289</sup>

Section 1201(f) of the Copyright Act contains the reverse engineering exception. United States case law on reverse engineering considers interoperability justifications but focuses

---

<sup>283</sup> 17 USC § 1201(e).

<sup>284</sup> As defined by 17 USC § 1201(f)(4).

<sup>285</sup> In *Sega Enterprises Ltd v Accolade Inc* 977 F 2d 1510 (9th Cir 1992), software reverse engineering was allowed. Other United States courts followed suit (Vinje op cit note 36 at 438).

<sup>286</sup> Mort op cit note 46 at 212.

<sup>287</sup> S Rep. 105-190 (1998) 32, cited Vinje op cit note 11 at 203.

<sup>288</sup> Supra note 285. This case permitted software reverse engineering in the United States and was followed by other American courts.

<sup>289</sup> S Rep 105-190 (1998) 32, cited by Vinje op cit note 11 at 203.

more broadly on the need for access to uncopyrightable functional principles embodied in computer software.<sup>290</sup> The reverse engineering exception in the Copyright Act, however, more closely resembles article 6 of the European Directive on the Legal Protection of Computer Programs,<sup>291</sup> which allows reverse engineering only for purposes of interoperability.<sup>292</sup> The language of the Directive, adopted in 1991, resulted from a compromise between competing factions of the computer industry who had long fought over the permissibility of software reverse engineering. So it seemed logical to include this language in the DMCA rather than to follow United States case law.<sup>293</sup>

Section 1201(f) contains a technology related exception to all the prohibitions in section 1201. It addresses the concern that software producers can include technological means in their computer programs to prevent not only unlawful copying but also the lawful copying inherent in software reverse engineering. Another company may then create a device to circumvent the reverse engineering ‘lock’, and so facilitate lawful recompilation for interoperability purposes. But that device may also be capable of being used to circumvent the protection system for purposes of unlawful reproduction. Put differently, although a device that circumvents a reverse engineering ‘lock’ clearly would have a lawful use, like many such devices it could also have unlawful uses. A company seeking to eliminate legitimate competition by preventing reverse engineering may then claim that the circumvention device (or perhaps even the reverse engineering itself) has the primary purpose of circumventing a mechanism that prohibits or inhibits the infringement of its rights.<sup>294</sup> Accordingly, unless properly limited, the prohibition on the circumvention of technical protection systems may allow companies to prevent, through technical means, reverse engineering that they cannot prevent through copyright law.<sup>295</sup>

Section 1201(f)(1) permits people who have ‘lawfully obtained the right to use a copy’ of a

---

<sup>290</sup> *Sega Enterprises Ltd v Accolade Inc* supra note 285.

<sup>291</sup> Council Directive of 14 May 1991 on the Legal Protection of Computer Programs, 91/250; see Pamela Samuelson ‘Comparing U.S. and E.C. Copyright Protection for Computer Programs: Are They more Different than They Seem?’ (1994) 13 *Journal of Law and Commerce* 279.

<sup>292</sup> Band & Isshiki op cit note 137 at 220; Cohen op cit note 232 at 239; Samuelson op cit note 291 at 279.

<sup>293</sup> Vinje op cit note 11 at 203.

<sup>294</sup> Software developers could even argue that merely distributing their programs in object code (rather than source code) constitutes a technological means of protection.

<sup>295</sup> Ginsberg op cit note 114 at 149; Vinje op cit note 36 at 438.

computer program to defeat the access code ‘for the sole purpose of identifying and analysing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs. . .’.<sup>296</sup> These elements must not previously have ‘been readily available’ to the person engaging in the decompilation (for example, in an unencrypted version of the computer program), and the acts of identification and analysis must not infringe the copyright in the computer program.

The circumvention devices must enable an ‘independently created computer program’ to interoperate with the protected work before the reverse engineering exception will apply. In *Lexmark International Inc v Static Control Components Inc*,<sup>297</sup> the defendant’s computer program (the program created by the so-called reverse engineering) was merely a copy of the plaintiff’s program and not independently created. The defendant could, therefore, not successfully raise this exception.

This exception does not allow reverse engineering for the production of non-infringing works that are not designed to be interoperative.<sup>298</sup> The ‘sole purpose’ of the circumvention must be to analyze elements necessary for achieving interoperability. Circumvention and circumvention devices enabling reverse engineering for other purposes remain unlawful. So it appears as if programmers are prohibited from circumvention when they are engaged in error correction, or when they are determining whether the target of the reverse engineering infringes their copyright.<sup>299</sup>

Section 1201(f)(2) allows people who engage in reverse engineering to develop the ‘technological means’ to circumvent technological protection measures, but the exception does not confer on them the right to distribute these circumvention devices. Also, the language of the exemption requires that the circumvention be for the ‘sole purpose’ of analyzing elements necessary for achieving interoperability.<sup>300</sup> Few useful reverse engineering tools can ever meet this standard, as they often serve more than one function, and

---

<sup>296</sup> 17 USC § 1201(f)(1)-(2).

<sup>297</sup> Supra note 71 at 970.

<sup>298</sup> Sheets op cit note 260 at 18.

<sup>299</sup> Band & Isshiki op cit note 137 at 221; Vinje op cit note 11 at 203.

<sup>300</sup> See also *Lexmark International Inc v Static Control Components Inc* op cit note 71 at 970.

if they can be used to circumvent access control, they may be used to circumvent copy control, too. Despite the section 1201(f) exception, section 1201(i) effectively destroys the lawful market for these technological means of circumvention. Scientists may well have to reinvent the wheel every time they attempt to reverse engineer a program.<sup>301</sup>

The reverse engineering exception came before the court in *Universal City Studios Inc v Reimerdes*.<sup>302</sup> The court held that section 1201(f) was for the benefit of the reverse engineer herself, and not for another person who merely disseminated the fruits of the reverse engineer's labour. Information acquired through reverse engineering could be made available to others only by the reverse engineer herself, and the right to make the information available extended only to dissemination 'solely for the purpose' of achieving interoperability. It did not apply to the public dissemination of the means of circumvention. In the present case, the defendants merely took DeCSS from another web site and posted it on their own. Also, interoperability must be the 'sole purpose' of the reverse engineering. The defendants did not post DeCSS solely to achieve interoperability with Linux. So the court ruled that the defendants could not avail themselves of this exception. Ginsberg<sup>303</sup> believes that the court also could have observed that if section 1201(f) were properly applied, the program that resulted from the reverse engineering did not itself circumvent access control.

#### **4.3.6.3.4 Encryption Research**

Section 1201 contains a technology related exception to the prohibition on the circumvention of access control – it permits the circumvention of access control measures, and the development of the technological means to do so, in order to identify flaws in and the vulnerabilities of encryption technologies.<sup>304</sup>

The reason for this exception was the concern that the prohibition on the circumvention of access controls could have unintended adverse consequences. Of particular concern was the possibility that the prohibition could chill legitimate research and testing in the field of

---

<sup>301</sup> Sheets op cit note 260 at 18-19.

<sup>302</sup> Supra note 72 at 319-320.

<sup>303</sup> Ginsberg op cit note 244 at 7.

<sup>304</sup> 17 USC § 1201(g).

encryption research, especially inquiries that targeted flaws and vulnerabilities in cryptographic systems for controlling access to copyright works.<sup>305</sup> Given the importance of encryption technology in protecting copyright works and in promoting electronic commerce, generally, the impact of the prohibition on research efforts was considered. Congress recognized that ‘[t]he development of encryption science requires ongoing research and testing by scientists of existing encryption methods in order to build on those advances, thus promoting encryption technology generally’.<sup>306</sup> A limited exception for purposes of encryption research was accordingly enacted.

Both the government and the Recording Industry Association of America (RIAA) gave statements of opinion that scientists studying access control technology were not subject to the DMCA.<sup>307</sup> These statements were made after major record labels, through the Secure Digital Music Initiative (SDMI), challenged hackers to break their technology. Several researchers succeeded. One of them, Edward Felten, a professor in computer science at Princeton, was threatened by the RIAA when he planned to give a lecture regarding his research. He proceeded with litigation against the RIAA even after he gave the lecture. The case ended when both the government and the RIAA gave statements that scientists studying access control technology were not subject to the DMCA.<sup>308</sup> But these are mere statements of opinion that are not enforceable in court.

Section 1201(g) creates two exceptions to the prohibitions contained in section 1201(a) – to permit the act of circumvention in the course of legitimate, good faith encryption research, and to permit the sharing of tools used to perform such research.

#### **(a) The permissible acts of encryption research**

---

<sup>305</sup> HR Rep No105-551 (1998) at 27; S Rep No 105-190 (1998) at 15; ‘Report to Congress: Joint Study of Section 1201(g) of the Digital Millennium Copyright Act’ op cit note 65.

<sup>306</sup> House of Representatives Committee on the Judiciary, 105th Congress, *Section-by-Section Analysis of HR 2281 as Passed by the United States House of Representatives on 4 August 1998*, p 16 (Comm Print Sept 1998), cited by Vinje op cit note 11 at 203.

<sup>307</sup> Brian Leubitz ‘Digital Millennium? Technological Protections for Copyright on the Internet’ (2003) 11 *Texas Intellectual Property Law Journal* 417 at 428; Electronic Frontier Foundation ‘Security Researchers Drop Scientific Censorship Case’, accessible at <[http://www.eff.org/IP/DMCA/Felten\\_v\\_RIAA/20020206\\_eff\\_felten\\_pr.html](http://www.eff.org/IP/DMCA/Felten_v_RIAA/20020206_eff_felten_pr.html)> (visited on 5 May 2002).

<sup>308</sup> Ibid.

Section 1201(g)(2) creates an exception to section 1201(a)(1)(A) of the Copyright Act. As the latter prohibition came into force only on 28 October 2000, this exception, too, became operative only on that date.<sup>309</sup> It permits an individual to circumvent a technological measure in the course of good faith encryption research provided that four requirements are satisfied:<sup>310</sup> (a) the encrypted copy must be ‘lawfully obtained’; (b) defeating the access code must be ‘necessary to conduct such encryption research’; (c) the researcher must have made a ‘good faith effort to obtain authorization’ from the author before the circumvention; and (d) the act of good faith encryption research must ‘not constitute infringement under this title or a violation of applicable law other than this section’.<sup>311</sup>

Encryption research is defined as ‘activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products’.<sup>312</sup> This definition prescribes the nature of the permitted activities – activities to identify and analyze the flaws and vulnerabilities of encryption technologies. It limits those activities to ones carried out for specified purposes – to advance the state of knowledge, or to assist in product development.

Out of apparent concern that ‘encryption research’ could degenerate into a pretext for indiscriminate hacking of access controls, this provision also attempts to restrict the class of people qualified for the exception by listing factors to consider:<sup>313</sup> whether the information derived from the research was disseminated to advance the knowledge or development of encryption technology or to facilitate infringement; whether the researcher is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced in the field of encryption technology; and whether the researcher timely notifies the author with the

---

<sup>309</sup> Report to Congress: Joint Study of Section 1201(g) of the Digital Millennium Copyright Act’ op cit note 65.

<sup>310</sup> In *Universal City Studios Inc v Reimerdes* supra note 72 at 320-321, this defence failed, as the defendants’ conduct did not satisfy these four requirements.

<sup>311</sup> 17 USC § 1201(g)(2)(D) expressly refers to the Computer Fraud and Abuse Act 18 USC. So the encryption research may not infringe the prohibition on circumvention, copyright law, the Computer Fraud and Abuse Act, or any other applicable law (Dorothy Schrader ‘Digital Millennium Copyright Act, PL 105-304: Summary and Analysis’ in John V Martin (ed) *Copyright: Current Issues and Laws* (2002) 131 at 136).

<sup>312</sup> 17 USC § 1201(g)(1)(A).

<sup>313</sup> 17 USC §1201(g)(3).

findings and documentation of the research.

#### **(b) The use of technological means for research activities**

Section 1201(g)(4) creates an exception to the prohibition on circumvention devices in section 1201(a)(2) of the Copyright Act. This exception permits a researcher to develop and use a circumvention device, to share such technology with a project collaborator, or to share such technology with someone verifying the researcher's work. This exception came into force immediately on the enactment of the DMCA, as did the accompanying prohibition.

A person, then, may develop and employ or provide to her collaborator the technological means to circumvent for the sole purpose of performing acts of good faith encryption research.

The encryption research community remained concerned that the procedures and limitations imposed by the exception would have a chilling effect on encryption research. Particularly disturbing was the ability to provide circumvention devices only to research collaborators as opposed to the general encryption research market. To address these concerns, the Act required the Register of Copyrights and the Assistant Secretary of Commerce for Communications and Information to report jointly within a year on the effect of the subsection on encryption research and the development of encryption technology; the adequacy and effectiveness of technological protection for works protected by copyright, and the protection of authors against unauthorized access to their encrypted copyright works.<sup>314</sup>

#### **4.3.6.3.5 The Protection of Minors**

Section 1201(h) of the Copyright Act was added to address the concerns of parents who seek to prevent their children from seeing inappropriate content on the Internet. Congress was persuaded that screening devices that parents employ to protect their children may include a 'component or part' that circumvents access control, but that these devices should be

---

<sup>314</sup> 17 USC § 1201(g)(5). See 'The Digital Millennium Copyright Act of 1998: U.S. Copyright Office Summary', op cit note 247; Vinje op cit note 11 at 203.

available if the ‘component or part’ is necessary to a device that ‘does not itself violate the provisions of this title’ and has the ‘sole purpose to prevent the access of minors to material on the Internet’.

Section 1201(*h*) is drafted very narrowly. It allows the development of circumvention components that would permit a parent to access a restricted site visited by her child.<sup>315</sup> The parental screening device should not have a dual purpose – to circumvent in order to block her children’s inappropriate access, and to circumvent in order to facilitate unpaid access.<sup>316</sup>

This exception allows a court applying the prohibition to a component or part of a technological protection measure to consider the necessity for its incorporation in technology that prevents access by minors to material on the Internet. Rather than stating a clear exception in respect of such component or part, section 1201(*h*) merely allows a court to consider whether the component or part has this beneficial purpose when the court applies section 1201. The provision does not, however, instruct a court what to do once it has determined that this is the purpose of the component or part in question. Section 1201(*h*) applies only if the component or part is included in a product which does not itself violate the provisions of Title I. So a stand-alone device intended to perform this function is not permitted. While section 1201(*h*) appears to permit the manufacture of such a device, it arguably does not permit the use of the component or part. This absurdity flows from the ambiguous manner in which the provision was drafted.<sup>317</sup>

Nimmer<sup>318</sup> believes that this exception was crafted prematurely – it addresses a problem that did not exist when the DMCA was passed. Then, there was ‘[a] variety of tools available . . . [to] allow parents to exercise control in a manner consistent with their own family values, of their children’s access to online materials’.<sup>319</sup> According to Nimmer, these tools afforded parents ample protection, without making them liable under section 1201. He believes that Congress added this specific exception because it was concerned that ‘*in the future*, any of

---

<sup>315</sup> Vinje op cit note 11 at 204.

<sup>316</sup> Ginsberg op cit note 114 at 151.

<sup>317</sup> Band & Isshiki op cit note 137 at 222.

<sup>318</sup> Nimmer op cit note 91 at 861.

<sup>319</sup> Ibid quoting S Rep No 105-90 (1998) 14.

these tools [might] incorporate a part or component which circumvented a technological protection measure'.<sup>320</sup>

#### 4.3.6.3.6 Personal Privacy

Section 1201(i) provides an exception to the prohibition on circumventing and trafficking in access controls. This provision addresses the significant privacy concerns raised by users of digital networks. Some web site operators have, without notifying users, engaged in the practice of collecting or disseminating information about the online activities of people who contact the web sites, for example, by sending 'cookies' to a user's hard drive.<sup>321</sup>

This exception permits circumvention when the technological measure, or the work it protects, is capable of collecting or disseminating personally identifying information about the online activities of a natural person. This exception applies only if the user is not provided with (a) adequate notice that information is being collected, and (b) the capability to prevent or restrict such collection or dissemination; and (c) if the circumvention has no other effect on the ability of any person to gain access to any work.

If, by contrast, the information gatherer provides 'conspicuous notice' of its information collection, and enables the user to restrict the collection or dissemination of personally identifying information, then the user may not circumvent.<sup>322</sup> Similarly, the right to circumvent is limited to identifying and disabling the undisclosed 'cookie' or similar device. It does not entitle the user to 'gain access to any work'.<sup>323</sup>

This exception renders the Copyright Act one of the few areas of American law that approaches the standards for data protection in the European Directive on the Processing of Personal Data.<sup>324</sup> The Copyright Act is silent, though, about personal identifying information

---

<sup>320</sup> Ibid.

<sup>321</sup> Ginsberg op cit note 114 at 151.

<sup>322</sup> 17 USC § 1201(i)(1)(B).

<sup>323</sup> 17 USC § 1201(i)(1)(C).

<sup>324</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, art 25.

collected in the course of a transaction with the author.<sup>325</sup>

Band<sup>326</sup> identifies the following problems with this provision. In the first instance, users may not circumvent to protect their privacy if the web site notifies them that it has implanted a ‘cookie’.<sup>327</sup> Accordingly, once users receive the notice, they must choose whether to sacrifice their privacy or to refrain from their online activity. Secondly, while this provision permits acts of circumvention to protect privacy, it does not specifically permit the development and distribution of the means of effecting that circumvention – it creates an exception to section 1201(a)(1) but not to section 1201(a)(2). It is not clear how users are expected to effect circumvention if developers are not permitted to manufacture and distribute circumvention devices.

Again Nimmer<sup>328</sup> objects to this exception on the basis that it regulates a problem that did not exist when the DMCA was passed. He argues that Congress acted on a motivation that lay in the future when it stated that ‘because of the privacy concerns expressed that existing *or future technologies may evolve* in such a way that an individual would have to circumvent a technological protection measure to protect his or her privacy, the Committee concluded that it was prudent to rule out any scenario in which section 1201 might be relied upon to make it harder, rather than easier, to protect personal privacy on the Internet’.<sup>329</sup>

#### **4.3.6.3.7 Security Testing**

Section 1201(j) provides an exception to the prohibition on the circumvention of access control in section 1201(a) of the Copyright Act. It adds to the encryption research exception a further exception for information security activities. This exception for security testing was added during the last days of the 105th Congress to resolve concerns related to the effect of the anti-circumvention provision on efforts to test ‘the security value and effectiveness of the technological measures’ employed to protect ‘the integrity and security of computers,

---

<sup>325</sup> Cohen op cit note 232 at 237.

<sup>326</sup> Band & Isshiki op cit note 137 at 222.

<sup>327</sup> A ‘cookie’ is a technological device that collects or disseminates personally identifying information reflecting the online activities of the user.

<sup>328</sup> Nimmer op cit note 91 at 861-862.

computer systems, or computer networks’.<sup>330</sup> Sometimes the only way to test the security of a computer system is to try to break into the system. The Congressional Conference Report draws an analogy between this and a consumer ‘installing [a] lock on the front door and seeing if it can be picked’.<sup>331</sup> The Conference Committee Report explains that –

‘the conferees were concerned that section 1201(g)’s exclusive focus on encryption-related research does not encompass the entire range of legitimate information security activities. Not every technological means that is used to provide security relies on encryption technology, or does so to the exclusion of other methods.’<sup>332</sup>

Section 1201(j) creates two exceptions to the prohibition on the circumvention of access control measure – the first to permit the act of circumvention, and the second the development of technological means for such circumvention, for the purpose of testing the security of a computer, computer system, or computer network if it is otherwise legal under applicable law.<sup>333</sup>

The concept ‘security testing’ is defined as obtaining access, with the authorization of the owner or operator of the computer system, to a computer, computer system, or computer network, for the sole purpose of testing, investigating, or correcting a potential or actual security flaw or vulnerability.<sup>334</sup> In determining whether this exception is applicable, the court is required to consider whether the information derived from the security testing was used solely to promote the security measures, and whether it was used or maintained so as not to facilitate infringement.<sup>335</sup> The development, production, or distribution of technological means for the sole purpose of performing permitted acts of security testing is allowed.<sup>336</sup>

This exception is not available to the technologically adept who unilaterally, without the

---

<sup>329</sup> *Idem* at 861-862 quoting S Rep No 105-190 (1998) 18.

<sup>330</sup> Vinje op cit note 11 at 203.

<sup>331</sup> HR Conf Rep No 105-796 (1998) 67, cited by Vinje op cit note 11 at 203.

<sup>332</sup> *Ibid.*

<sup>333</sup> Again the circumvention may not violate the Computer Fraud and Abuse Act of 1986.

<sup>334</sup> 17 USC § 1201(j)(1).

<sup>335</sup> 17 USC § 1201(j)(3).

owners' permission, breaks into systems to warn the owners of the systems' vulnerabilities.<sup>337</sup>

In *Universal City Studios Inc v Reimerdes*,<sup>338</sup> the court rejected the defendants' attempt to invoke this exception – there was no evidence that DeCSS had anything to do with security testing or that the defendants' activities were authorized.

### 4.3.7 Remedies

#### 4.3.7.1 Civil Remedies

Any person injured by a violation of section 1201 or 1202 may bring a civil action in a Federal Court.<sup>339</sup> Section 1203 does not require that a person should have suffered damage – it merely requires that a person should be injured. This provision gives courts the power to grant a range of equitable and monetary remedies similar to those available for copyright infringement. The principal civil remedies available for a violation of section 1201 are temporary and permanent injunctions, and damages.<sup>340</sup>

The court has a discretion to reduce or remit damages in the event of innocent violation, where the violator proves that she was not aware and had no reason to believe that her acts constituted a violation. Pinnisi<sup>341</sup> believes that this is an exemption to the civil penalties for an 'innocent violator' who can prove that she did not know that her act constituted a violation. This does not mean that she did not violate the prohibitions – it merely means that the court can exempt her from the payment of damages. Therefore, although intent is not expressly required for civil liability, innocent violators can still be excused. It seems, then, as if intent (or at least negligence) is required for civil liability.

---

<sup>336</sup> 17 USC § 1201(j)(4).

<sup>337</sup> Ginsberg op cit note 114 at 149.

<sup>338</sup> Supra note 72 at 320-321.

<sup>339</sup> 17 USC § 1203.

<sup>340</sup> Besek op cit note 20 at 400.

<sup>341</sup> Chris Pinnisi 'Anti-Circumvention Law May Circumvent Fairness' (2002) 19 *Computer and Internet Lawyer* 5 at 6.

Special protection is given to non-profit libraries, archives, and educational institutions. They are entitled to a complete remission of damages where the institution in question ‘was not aware and had no reason to believe that its acts constituted a violation’.<sup>342</sup>

#### 4.3.7.2 Criminal Offences and Penalties

Before the enactment of the DMCA, there was legislation in place that could be used to obtain criminal convictions for copyright infringement. Such legislation included the Copyright Act and the No Electronic Theft Act of 1997.<sup>343</sup> Where computers are involved and copyright infringement as such cannot be proven, the unauthorized distribution of content can often be punished through proving wire fraud or electronic theft in contravention of the Wire Fraud Act.<sup>344</sup>

Criminal penalties for copyright violations are not foreign to American law. It is a criminal offence to violate section 1201 or 1202 wilfully and for purposes of commercial advantage or private financial gain. A fine of up to \$500 000 or up to five years’ imprisonment may be imposed for a first offence, and a fine of up to \$1 million or up to 10 years’ imprisonment may be imposed for subsequent offences.<sup>345</sup> It is important to note that only wilful violations for purposes of commercial advantage or private financial gain<sup>346</sup> are punishable. As wilfulness (intent) is expressly required for criminal liability, innocent violators go free.

The requirement of ‘wilfulness’ relates to the violation of section 1201 and not to the copyright infringement. Section 1204 does not demand any inquiry into the *motive* for circumvention. Section 1201(a)(2) and 1201(b) can be violated without the perpetrator having the motive or intention that the device she is dealing with be used for infringing purposes.<sup>347</sup> Once a person deals with circumvention devices for commercial advantage or private financial gain, she wilfully violates these provisions, despite the absence of the

---

<sup>342</sup> 17 USC § 1203(c)(5)(B).

<sup>343</sup> Codified in scattered sections of 17 and 18 USC.

<sup>344</sup> 18 USC § 1343; see Pennisi op cit note 341 at 5.

<sup>345</sup> 17 USC § 1204.

<sup>346</sup> 17 USC § 1204(a).

<sup>347</sup> This was reiterated in *Universal City Studios Inc v Reimerdes* supra note 72 at 319: ‘the offering or provision of the program [the circumvention device] is the prohibited conduct – and it is prohibited irrespective of why

intention that they be used to infringe copyright.

According to Pennisi,<sup>348</sup> it seems as if the DMCA imposes strict criminal liability for dealing in circumvention devices – it imposes a blanket punishment on *all* intentional circumvention irrespective of motive.<sup>349</sup> This absolute prohibition on devices ignores the fact that no criminal liability exists for the distribution of other instruments used to commit traditional copyright infringement.

Non-profit libraries, archives, and educational institutions are entirely exempted from criminal liability.<sup>350</sup>

In *Department of Justice, Indictment US v Elcom and Dmitry Sklyarov*<sup>351</sup> the first indictment under the anti-circumvention provision of the Copyright Act was filed.<sup>352</sup> However, as a result of an agreement between the United States Attorney's Office for the Northern District of California and Sklyarov,<sup>353</sup> the case against him was terminated. Still, Pennisi<sup>354</sup> believes that the premature termination of the case against Sklyarov suggests that there is an overreach problem with the present wording of section 1204.

#### **4.3.8 Summarizing the Objections Against the DMCA Amendments**

The following objections, most of which I have discussed earlier in this chapter, were raised against the provisions of section 1201.

##### **4.3.8.1 Section 1201 Will Promote the Digital Lockup of Copyright Works**

---

the program was written.'

<sup>348</sup> Pennisi op cit note 341 at 6-7.

<sup>349</sup> Idem at 6.

<sup>350</sup> 17 USC § 1204(b).

<sup>351</sup> Criminal No 5-01-257P (ND Cal Filed 2001); see further 'Panel III: Implications of Enforcing the Digital Millennium Copyright Act: A Case Study, Focussing on United States v Sklyarov' (2002) 12 *Fordham Intellectual Property, Media and Entertainment Law Journal* 805 at 806n2.

<sup>352</sup> The defendant was charged with contravening 17 USC § 1201(b)(1)(A) and 18 USC § 2.

<sup>353</sup> In terms of this agreement, the defendant agreed to cooperate with the United States in its ongoing prosecution of his former employer, ElcomSoft Co Ltd.

<sup>354</sup> Pennisi op cit note 341 at 7.

Access constraints existed in the analogue world through distribution methods and copying technology). But these constraints were very different from those on access through the protection of access control technologies. These technologies enable authors to control not only initial access but also each subsequent access. Access controls can also prevent acts such as reading or browsing that were permissible in the analogue world. So the protection of access controls created the fear that authors would lock up their works or require payment for each access to their works, which would make it impossible for users to browse or view the protected works.

Also, by locking up their works, authors would prevent users from accessing these works in order to make fair use of them.

Even where a work exist in an alternative format, the exercise of a privilege in relation to an alternative format may be so inconvenient that it can, practically, be regarded as impossible. Such works would be digitally locked up despite the existence of alternative formats.<sup>355</sup>

#### **4.3.8.2 Section 1201 Will Promote the Digital Lockup of Works in the Public Domain**

The prohibitions on circumvention and on the trafficking in circumvention devices are not dependant on subsequent copyright infringement. When works in the public domain are protected by technological protection measures, they become inaccessible, as any circumvention contravenes section 1201. Also, as is the case with works protected by copyright, it may be so inconvenient to access an alternative format of a work in the public domain that it can becomes impossible to do so. Even in these circumstances circumvention is be prohibited.

#### **4.3.8.3 Section 1201 Inhibits Non-infringing Use**

It is impossible to make fair use of a work without first accessing it. So the prohibition on the act of circumvention inhibits not only the ability to access works but also to use them The exceptions to this prohibition are inadequate to allow non-infringing use.

#### **4.3.8.4 The Device Prohibitions Eliminate the Ability to Make Non-infringing Use**

This objection goes hand in hand with the previous one. Even users who, in terms of an exception, would be allowed to circumvent, would not have the means with which to circumvent because of the prohibitions on the trafficking in circumvention devices.

#### **4.3.8.5 The Device Prohibitions Could Lead to a Two-fold Liability**

A person trafficking in circumvention devices can be held liable for a contravention of the anti-trafficking provisions of section 1201, and for contributory copyright infringement under section 1201(c)(2).

#### **4.3.8.6 Section 1201 Will Lead to a Pay-per-use Society**

The protection of technological measures makes it possible to enforce measures that would require payment for every access to a work. This could result in a situation in which no use of a copyright work would be free. Even users wanting to make non-infringing use of a work could now be required to pay for such non-infringing use, since use would be impossible without access, and access would require payment.

#### **4.3.8.7 The Rule-making Powers of the Librarian of Congress May Lead to Uncertainty**

In the first instance, the rule-making process requires the Librarian of Congress and the Registrar of Copyrights to predict the future, and so the process is speculative. Secondly, the exemptions differ from period to period, which creates uncertainty as to whether or not a particular class of works is actually exempted. Thirdly, these exemptions cannot be raised as a defence against an action for copyright infringement.

#### **4.3.8.8 Section 1201 Allows Authors to Defeat Privileges under the First-sale Doctrine**

---

<sup>355</sup> Besek op cit note 20 at 481.

The first sale doctrine allows a lawfully obtained physical object containing a copy of a copyright work to be given away or sold, but it does not allow the digital transmission of an electronic copy over a computer network.<sup>356</sup> However, critics contend that access controls limiting copies of digital works to use on a particular playback device (such as a computer) or a particular platform (such as regionally licensed DVD players) may deprive users of their privileges under the first sale doctrine. This fear is not unfounded. Besek<sup>357</sup> recognizes the possibility that the first sale doctrine may be compromised when a work is distributed in a physical medium but its use is limited to certain specific machines, such as the particular computer on which the work is downloaded.

With regards to the limitation to particular platforms, the Copyright Office rejected the notion that requiring copies of works to be played on a particular platform interferes with user privileges under the first sale doctrine. This means that the Office accepts the decisions in *Universal City Studios Inc v Corley*<sup>358</sup> and *Sony Computer Entertainment America Inc v Gamemasters*.<sup>359</sup> So far, under the rule-making procedure, the Office has rejected requests for an exemption to enable platform shifting.<sup>360</sup> The Office maintains that ‘[r]egion coding imposes, at most, an inconvenience rather than actual or likely harm, because there are numerable options available to individuals seeking access to content from other regions.’<sup>361</sup> A user would, therefore, not be allowed to bypass access controls on a legitimately obtained copy of a work in order to use it on a playback device obtained in another geographical area.

#### **4.3.8.9 Section 1201 Prevents Legitimate Research Activities**

Some argue that the exceptions for reverse engineering and encryption research are not broad enough to meet legitimate research needs.

---

<sup>356</sup> United States Copyright Office DMCA Section 104 Report 86 (2001), accessible at <<http://www.copyright.gov/reports/studies/dmca/sec-104-report-vol-1-pdf>>, cited by Besek op cit note 20 at 423 & 473.

<sup>357</sup> Besek op cit note 20 at 473.

<sup>358</sup> 272 F 2d. 429 (2nd Cir 2001).

<sup>359</sup> Supra note 77.

<sup>360</sup> Besek op cit note 20 at 473, esp notes 370 & 504.

#### **4.3.8.10 Section 1201 Restricts Competition in the Replacement Parts Market**

This objection is based on the decisions in *Lexmark International Inc v Static Control Components Inc*<sup>362</sup> and *The Chamberlain Group Inc v Skylink Technologies Inc*,<sup>363</sup> where the plaintiffs relied on the anti-circumvention provisions to restrict competition in the replacement parts market.

#### **4.3.8.11 Section 1201 Is Unconstitutional**

Some critics believe that section 1201 is unconstitutional, as it inhibits free speech and violates the First Amendment. Circumvention software is speech, so the argument goes, and limiting its distribution is an impermissible content-based restriction, which violates the First Amendment. The prohibition on circumvention devices further violates the First Amendment, as users need these devices to exercise their fair use privileges.<sup>364</sup>

The constitutionality of the authority of the Librarian of Congress to exempt classes of works from the prohibition on the act of circumventing access controls is also questioned. However, as the Librarian's authority has not yet been contested, this objection is of little practical relevance.

#### **4.3.8.12 Section 1201 Will not Succeed in Effectively Limiting Infringement**

The anti-circumvention approach of the DMCA can never be effective in limiting copyright infringement. This is quite simply because the enforcement of the prohibition on the act of circumvention will require lawsuits against each private individual infringer, who could be situated anywhere in the world.<sup>365</sup> Also, prohibited circumvention devices are readily available to those who would wish to circumvent, and even those who do not want to

---

<sup>361</sup> Federal Register: 27 November 2006 op cit note 201 at 68478.

<sup>362</sup> Supra note 71.

<sup>363</sup> Supra note 115.

<sup>364</sup> In *Universal City Studios Inc v Corley* supra note 264 at 458; *United States v Elcom Ltd* supra note 125, and *321 Studios v Metro Goldwyn Mayer Studios Inc* supra note 75 at 1101-1103), this argument was raised but dismissed.

<sup>365</sup> Lunney op cit note 85 at 830.

circumvent can easily obtain clear, unencrypted copies of copyright works on peer-to-peer networks.<sup>366</sup>

#### 4.4 Conclusion

Section 1201 of the Copyright Act goes far beyond the WCT. The WCT does not require any of the broad provisions of section 1201. The WCT does not speak of devices; it only speaks of circumvention. It is silent on the prohibition of circumvention in the absence of infringement. Indeed, it seems as if the WCT prohibits only circumvention that actually results in infringement.<sup>367</sup>

Section 1201 also radically departs from traditional copyright law principles. For the first time, copyright law now regulates technology rather than actions. Section 1201 creates an action independent of copyright infringement, which leads authors like Sheets<sup>368</sup> to argue that the DMCA is not even properly part of the Copyright Act. The prohibitions in section 1201 are also not subject to traditional copyright exceptions. Lastly, the protection of access controls against circumvention indirectly creates an entirely new right, an access right, which is likewise unlimited by traditional copyright defences.

The DMCA created a technological monopoly in favour of authors. Authors can now protect their works as they seem fit by using technological protection measures, which enables them to determine the scope of copyright protection.<sup>369</sup> This implies that the scope of protection is determined by those with a monetary interest in the protection of their works rather than by an independent judiciary.

However, the most far-reaching consequence of the anti-circumvention provisions is that they have the potential to eliminate non-infringing uses of those copyright works protected by technological measures. The broad prohibition and narrowly crafted exceptions will make circumvention impossible for any use not expressly and specifically excepted. Even in those

---

<sup>366</sup> Besek op cit note 20 at 469.

<sup>367</sup> Band & Isshiki op cit note 137 at 225.

<sup>368</sup> Sheets op cit note 260 at 20.

instances where the act of circumvention is allowed, the prohibition on devices will render it impossible to perform such non-infringing acts.

There are only three ways in which non-infringing uses can possibly be saved. In the first instance, the courts can declare the anti-trafficking provisions unconstitutional. Secondly, the courts can develop a new common-law fair use exception to the anti-trafficking provisions. Thirdly, Congress can draft a fair use exception to the anti-trafficking provisions that will withstand constitutional scrutiny.<sup>370</sup>

In several cases the constitutionality of the DMCA was contested.<sup>371</sup> Although these decisions rejected the First Amendment challenges, it still does not mean that the DMCA is immune to such challenge. For the time being, though, one has to proceed on the basis that the DMCA is constitutional.

In none of the decided cases have the courts sought to formulate a common-law exception of fair use. But what they have done is to move away from the earlier very narrow interpretations given to section 1201 in cases such as *Universal City Studios Inc v Corley*,<sup>372</sup> *321 Studios v Metro Goldwyn Mayer Studios Inc*,<sup>373</sup> and *Sony Computer Entertainment America Inc v Gamemasters*.<sup>374</sup> In *Lexmark International, Inc v Static Control Components Inc*<sup>375</sup> and *The Chamberlain Group Inc v Skylink Technologies Inc*,<sup>376</sup> for example, the courts followed a broader interpretation of the anti-circumvention provisions, having regard to the rights of users and competitors.

Finally, on 21 March 2002, Senator Fritz Hollings introduced the Consumer Broadband and Digital TV Promotion Bill.<sup>377</sup> However, this Bill is drafted in the same vein as the DMCA

---

<sup>369</sup> Lunney op cit note 85 at 841 and 843.

<sup>370</sup> Van den Elzen op cit note 120 at 702.

<sup>371</sup> *Universal City Studios v Reimerdes* supra note 72 at 325-33; *Universal City Studios v Corley* supra note 264 at 435-55; *United States v Elcom Ltd* supra note 125 at 1127-32; *321 Studios v Metro-Goldwyn-Mayer Studios* supra note 75 at 1099-1101.

<sup>372</sup> Supra note 358 at 444.

<sup>373</sup> Supra note 75 at 1093-1096.

<sup>374</sup> Supra note 77 at 981, 987 and 990.

<sup>375</sup> Supra note 71.

<sup>376</sup> Supra note 115.

<sup>377</sup> Consumer Broadband and Digital TV Promotion Act of 2002 S. 2048, 107th Congress, 2d Session. Full text

and so is not of much help to users. It promises that the increased protection of copyright works online will lead to greater confidence in and subscription to the new broadband and digital television technologies.<sup>378</sup> But, despite its claim to protect the privileges for legitimate consumer copying in the home,<sup>379</sup> it further restricts users' privileges to make private copies. It also proposes to prevent illegal transmissions of content over the Internet by requiring all digital receivers, recorders, and players to be equipped with a government technology standard.

There has been wide criticism of the Hollings Bill since its introduction.<sup>380</sup> In the first instance, it assumes that the Government will act quickly enough to develop and introduce a technology standard applicable to all proposed media devices. Secondly, the Bill assumes that the technology standard it requires will work. But what if it does not? Thirdly, the consumer copying provision in the Bill does not assure consumers that they will be able to make full and fair use of the digital content that they purchase.

Three other Bills were also introduced.

In direct response to the negative effect of the DMCA and the Consumer Broadband and Digital TV Promotion Act of 2002<sup>381</sup> on users' privileges, Congressman Rick Boucher introduced HR 107, entitled the 'Digital Media Consumers' Rights Act of 2003'.<sup>382</sup> Although this Bill addresses technological protection measures only indirectly, it proposes direct amendments to the DMCA amendments to restore fair use privileges. Under the heading 'Fair Use Restoration', clause 5(a) contains an exception to permit trafficking in circumvention devices if the person 'is acting solely in furtherance of scientific research into technological protection measures'. Clause 5(b) contains a broad exception to allow the circumvention of a technological protection measure 'in connection with the access to, or the use of, a work if such circumvention does not result in an infringement of the copyright in the

---

accessible at <http://thomas.loc.gov/cgi-bin/query/z?c107:S.2048>: (last visited on 28 February 2007).

<sup>378</sup> Section 2.

<sup>379</sup> Section 3(e)(2).

<sup>380</sup> Joe Kraus, Testimony to the House Energy and Commerce Committee (Apr. 25, 2002), accessible at <<http://www.digitalconsumer.org/testimony-20020425.html>> (visited on 20 March 2007)

<sup>381</sup> Op cit note 377.

<sup>382</sup> HR 107, 108th Congress, 1st Sess (2003).

work'. The Bill also seeks to amend the anti-trafficking provisions of section 1201(a)(2) and 1201(b) of the Copyright Act to allow the manufacture, distribution, or making non-infringing use of a hardware or software product 'capable of enabling significant non-infringing use of a copyrighted work'. This amendment would bring the Copyright Act back in line with the *Sony* decision,<sup>383</sup> which established the 'substantial non-infringing use' standard for copying devices. Clause 24A tackles copy-protected compact discs by requiring their labels to inform consumers if their fair use rights will be restricted by the technological protection measures encoded in the product. The information that must be printed on the packaging includes any restrictions on the number of times that a song file may be downloaded to a computer, and the minimum recommended software requirements for playback of the songs on a computer.

On 4 March 2003, Representatives Boucher and Lofgren introduced HR 1066,<sup>384</sup> entitled the 'Benefit Authors without Limiting Advancement of Net Consumers Expectations Act of 2003'. Section 5 of this Bill (headed 'Permissible Circumvention to Enable Fair Use and Consumer Expectations') would allow circumvention of access or rights control measures on lawfully obtained copies of a work, if such act is necessary to make non-infringing use of a work, and the author fails to make publicly available the necessary means to make non-infringing use without additional cost or burden to the user.<sup>385</sup> The Bill also provides that it would not be an infringement to manufacture, distribute, or otherwise traffic in technological means to circumvent access or copy control, if such means are necessary to make a non-infringing use, and the author fails to make available the necessary means to make such use without additional cost or burden to the user.<sup>386</sup>

H.R. 1066 allows a user to circumvent only if the author fails to provide the 'necessary means' to exercise fair use. But the means must be made available to users 'without additional cost or burden'. It seems as if this condition allows users to circumvent if the

---

<sup>383</sup> *Sony Corp of Am v Universal City Studios Inc* supra note 5.

<sup>384</sup> Benefit Authors without Limiting Advancement of Net Consumers Expectations Act of 2003, H.R. 1066, 108th Congress (2003). Full text accessible at < <http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.1066:IH>> (visited on 28 February 2007).

<sup>385</sup> Section 5(1).

<sup>386</sup> Section 5(2).

available means is not convenient. Besek<sup>387</sup> also argues that the requirement that the author provide ‘necessary means’ to make non-infringing use is ambiguous. Does this, for example, connote the means necessary to make copies, and if so, how many copies?

The phrase ‘necessary means’ is the standard used in article 6.4 of the Copyright Directive of the European Union. But HR 1066 is far broader than the Directive. Under the Directive, where authors do not make the means available, the responsibility to do so is left to the Member States and not to individual users. The Directive requirement attaches only to a number of exceptions, and not all non-infringing uses. Also, the ‘means mandate’ of the Directive does not apply to on-demand services.<sup>388</sup>

So HR 1066 would broaden exceptions to copyright, and, as a result of its amendment of section 1201, the circumstances in which circumvention would be permitted. From the above it is clear that HR 107 and HR 1066 both deliberately seek to reverse the DMCA approach.

S 1621, titled the ‘Consumers, Schools and Libraries Digital Rights Management Awareness Act’,<sup>389</sup> was introduced by Senator Brownback on 16 September 2003. It proposes, among other things, to create a broad digital first sale privilege: it would grant owners of digital media products the right to dispose of their copies or transmissions, provided that the originals are deleted.<sup>390</sup> The term ‘digital media products’ include copies of copyright works distributed to the public in digital form, either electronically or fixed in a physical medium.<sup>391</sup> The Bill prohibits the use of access control that limit consumers’ ability to transfer digital media products through transmission, donation, or resale.<sup>392</sup>

American users struggle to keep head above the DMCA waters. After the strict interpretations of section 1201 in *Universal City Studios Inc v Corley*,<sup>393</sup> *321 Studios v Metro*

---

<sup>387</sup> Besek op cit note 20 at 482.

<sup>388</sup> Idem at 483.

<sup>389</sup> Consumers, Schools and Libraries Digital Rights Management Awareness Act of 2003, S. 1621, 108th Congress (2003). Full text available at <<http://thomas.loc.gov/cgi-bin/query/z?c108:S.1621>: > (visited on 28 February 2007).

<sup>390</sup> Section 6(a).

<sup>391</sup> Section 9(3).

<sup>392</sup> Section 6(c).

<sup>393</sup> Supra note 358 at 444.

*Goldwyn Mayer Studios Inc*,<sup>394</sup> and *Sony Computer Entertainment America Inc v Gamemasters*<sup>395</sup> it seemed as if drowning was inevitable. But all hope is not lost: *Lexmark International, Inc v Static Control Components Inc*<sup>396</sup> and *The Chamberlain Group Inc v Skylink Technologies Inc*<sup>397</sup> re-established the copyright balance by giving broader interpretations to section 1201, having regard to user privileges. Three proposed Bills attempt to do the same.

---

<sup>394</sup> Supra note 75 at 1093-1096.

<sup>395</sup> Supra note 77 at 976, 981 and 990.

<sup>396</sup> Supra note 71.

<sup>397</sup> Op cit note 115.

## CHAPTER 5: THE EUROPEAN UNION

‘Poor Alice! It was as much as she could do, lying down on one side, to look through into the garden with one eye; but to get through was more hopeless than ever: she sat down and began to cry again.’

LEWIS CARROL

*Alice’s Adventures in Wonderland*

### 5.1 Introduction

In contrast to the philosophical incentive approach followed in the United States, European copyright jurisprudence is based on the natural rights theory.<sup>1</sup> It sees copyright as arising from the personality rights of the individual creator of the subject matter. Protection is given out of respect for the author’s creative act and extends beyond the mere economic rights to include moral rights.<sup>2</sup> Article 27(2) of the Universal Declaration of Human Rights thus also states that ‘[e]veryone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author’.

The natural rights theory of copyright is stated by Willes J in *Millar v Taylor*:<sup>3</sup> ‘It is certainly not agreeable to natural justice that a stranger should reap the beneficial pecuniary produce of another man’s work.’ According to the natural rights theory, an author’s rights to her work should be indefinite and all-embracing. It supports granting authors full control over their works and the maximum possible market return from the exploitation of those works.

The European Community (EC) and its Member States share legislative competence in the area of copyright law.<sup>4</sup> The legislative powers of the EC in the field of intellectual property

---

<sup>1</sup> Simon Fitzpatrick ‘Copyright Imbalance: U.S. and Australian Responses to the WIPO Digital Copyright Treaty’ [2000] *European Intellectual Property Review* 214 at 216.

<sup>2</sup> Jacqueline Lipton ‘Copyright in the Digital Age: A Comparative Survey’ (2001) 27 *Rutgers Computer and Technology Law Journal* 333 at 335.

<sup>3</sup> 4 Burr 2303 (1769).

<sup>4</sup> Patrick Ravillard ‘Towards a European Directive on Enforcement of Intellectual Property Rights’ (2001) 136 *Trademark World* 40; Jörg Reinbothe & Silke von Lewinski ‘The WIPO Treaties 1996: Ready to Come into

originate in articles 47.2, 55, and 95 of the Treaty Establishing the European Community.<sup>5</sup> The preamble of the Copyright Directive<sup>6</sup> expressly refers to these provisions in the Treaty. While it is expected of EC Member States to act consistently with EC legislation, EC law does not automatically override national legislation. In the area of intellectual property law, an EC directive usually recommends and gives effect to general aims. Member States then have to comply with the directive by enacting their own national legislation.<sup>7</sup>

The assembly established under article 15 of the WIPO Copyright Treaty (WCT) may decide to admit certain intergovernmental organizations to become party to the treaty,<sup>8</sup> and has so admitted the European Community.<sup>9</sup> So both the EC itself and its Member States became parties to the WCT.<sup>10</sup> The implementation of the WCT in the European Community took place on two levels. On the first level, the EC legislature had to issue a directive covering the areas of Community competence,<sup>11</sup> which then, at the second level, had to be implemented by EC Member States at national level. At the same time, Member States had to legislate themselves on those areas of the treaty that remained part of their national competence.<sup>12</sup> So the implementation of the WCT into the laws of the EC Member States does not serve as a typical example of the implementation of the WCT into national law.<sup>13</sup>

The EC implemented the provisions of the WCT by providing much broader copyright protection than required by the WCT. In a sense this is justified by the traditional natural

---

Force' [2002] *European Intellectual Property Review* 199 at 202.

<sup>5</sup> Concluded in Rome on 25 March 2007. See P Bernt Hugenholtz 'Why the Copyright Directive Is Unimportant, and Possibly Invalid' [2000] *European Intellectual Property Review* 499 at 501, who refers to a judgment of the European Court of Justice (ECJ 5 October 2000 Case C-376/98 (*Germany v European Parliament and Council of the EU*)) and questions the validity of the Copyright Directive in view of the provisions of the EC Treaty.

<sup>6</sup> Directive 2001/29/EC of the European Parliament and the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society [2001] O.J. L167/10. Full text available at <[http://europa.eu.int/documents/comm/index\\_en.htm](http://europa.eu.int/documents/comm/index_en.htm)> (visited on 11 March 2004) (the 'Copyright Directive').

<sup>7</sup> Lipton op cit note 2 at 335-336.

<sup>8</sup> Article 17.2 of the WCT.

<sup>9</sup> Article 17.3 of the WCT.

<sup>10</sup> Silke von Lewinski 'Proposed EC Directive on Copyright and Related Rights in the Information Society as It Progresses' (1999) 30 *ICC* 767 at 768.

<sup>11</sup> Reinbothe & Von Lewinski op cit note 4 at 202.

<sup>12</sup> Such as the provisions on the performers' moral rights (Lewinski op cit note 10 at 768; Reinbothe & Lewinski op cit note 4 at 202).

<sup>13</sup> Reinbothe & Lewinski op cit note 4 at 202.

rights approach. Stronger protection also seemed necessary to protect the EC's trade interests, because the EC, like the United States, belongs to the copyright exploiting block.

I shall limit my discussion here to the implementation of the WCT at EC directive level.<sup>14</sup>

## 5.2 Preparations for Law Making in the Information Era

Some of the issues covered by the WCT had already been dealt with by earlier EC directives. A new directive was needed to cover only the following aspects of the WCT: the right of communication to the public and making available to the public, the general distribution right, the protection of technological protection measures, and the protection of rights management information.<sup>15</sup> I shall confine this discussion to the protection of technological protection measures.

The Commission believed that technological protection measures had to be protected at EC level, because it feared that if Member States legislated on this issue individually, then conflicting legal provisions would create practical problems.<sup>16</sup>

The first step towards implementing legal measures for the protection of technological protection measures in EC legislation was the EC Green Paper on Copyright and Related Rights in the Information Society.<sup>17</sup> This Paper was followed by the EC Proposal for the Protocol to the Berne Convention,<sup>18</sup> and the EC Follow-up Paper to the Green Paper on Copyright and Related Rights in the Information Society.<sup>19</sup>

---

<sup>14</sup> The Follow-up to the Green paper recognized the need for implementation on EC level: 'A large consensus exists that legislative action should be undertaken *at Community level* in order to avoid barriers which might hamper the proper functioning of the Single Market. In so doing, the Commission should take the international minimum standards into account, which are currently being negotiated under the auspices of WIPO' (emphasis added).

<sup>15</sup> Reinbothe & Lewinski op cit note 4 at 202.

<sup>16</sup> Recital 26, cited by Karen Murray 'The Draft Directive on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society' (1998) 9 *Entertainment Law Review* 190 at 192.

<sup>17</sup> COM(1995)382 accessible at <<http://www.eblida.org/ecup/lex/com95382.org>> (visited on 31 March 2003) ('The Green Paper').

<sup>18</sup> The full text of the EC Proposal is available at <<http://mailman.anu.edu.au/pipermail/link/1996-July/024547.html>> (visited on 28 March 2007) (the 'EC Proposal').

<sup>19</sup> COM(1996)568 available at <<http://www.eblida.org/ecup/lex/com96586.html#23>> (visited on 30 March 2004) (the 'Follow-Up Paper').

On 10 December 1997, the European Commission presented a Proposal for a European Parliament and Council Directive on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society.<sup>20</sup> The Commission then submitted an amended proposal<sup>21</sup> on 21 May 1999, and the European Council of Ministers reached a Common Position on 28 September 2000. The Copyright Directive was adopted on 22 May 2001.<sup>22</sup>

### **5.2.1 The European Community Green Paper of July 1995 on Copyright and Related Rights in the Information Society<sup>23</sup>**

The term ‘information society’ was first used in the European Commission’s White Paper – *Growth, Competitiveness, Employment - the Challenges and Ways Forward into the Twenty-first Century*. Drawing on the conclusions of the White Paper, a working party compiled a report for the European Council, entitled *Europe and the Global Information Society - Recommendations of the High-level Group on the Information Society to the Corfu European Council*.<sup>24</sup> This report identified intellectual property protection as a key issue in the development of the information society. The protection of intellectual property rights were seen as a fundamental part of the regulatory system needed to establish the information society. The Commission subsequently adopted a communication, entitled *Europe’s Way to the Information Society: an Action Plan*,<sup>25</sup> that set the framework for action by the Commission and cleared the way for more specialized discussion papers on specific subjects, such as the protection of intellectual property rights.<sup>26</sup>

This Communication was followed by *The European Community Green Paper of July 1995*

---

<sup>20</sup> COM(1997)628/FINAL (‘The Proposal’).

<sup>21</sup> Amended Proposal for a European Parliament and Council Directive on the harmonisation of certain aspects of copyrights and related rights in the Information Society, doc COM(1999)250/FINAL of 21 May 1999, [1999] OJ C180/6 (the ‘Amended Proposal’).

<sup>22</sup> For a general discussion of the legislative procedure, see Alvisè Maria Casellati ‘The Evolution of Article 6.4 of the European Information Society Copyright Directive’ (2001) 24 *Columbia-VLA Journal of Law & The Arts* 369 at 372, especially at note 7.

<sup>23</sup> The Green Paper op cit note 17.

<sup>24</sup> Brussels, 26 May 1994.

<sup>25</sup> Communication from the Commission to the Council and the European Parliament and to the Economic and Social Committee and the Committee of Regions, COM(94) 347/FINAL, Brussels, 19 July 1994.

<sup>26</sup> See The Green Paper op cit note 17, Introduction para 1–9.

on *Copyright and Related Rights in the Information Society*<sup>27</sup> (the ‘Green Paper’). (A green paper is a discussion paper published by the Commission on a specific policy area. Primarily it is a document that sets out a range of ideas and invites interested parties to participate in a process of consultation and debate.<sup>28</sup>) The European Commission adopted the Green Paper on 19 July 1995.<sup>29</sup> Its objective is to provide the background to a number of questions relating to copyright and related rights where legislative measures may be needed as the information society develops.<sup>30</sup> The Green Paper provided the impetus for the Copyright Directive.

The Green Paper is divided into two chapters. Chapter One deals with the reasons for producing the Green Paper, the issues involved, and the legal framework of the Information Society as it existed at the time of the drafting of the Green Paper. It sets out to describe how the Information Society should function.<sup>31</sup> Chapter Two elects nine of the points regarding copyright and related rights that were raised in contributions from interested parties, which the Commission believes should be given priority to ensure that the information society can function properly.<sup>32</sup> Part One of Chapter Two deals with general questions, Part Two with specific rights, and Part Three with issues relating to the exploitation of rights.<sup>33</sup>

Section IX of Part Three is devoted to ‘Technical Systems of Protection and Identification’. The first paragraph contains a description of existing technological systems or those under development,<sup>34</sup> and the second paragraph refers to the law as it existed at the time of the drafting of the Green Paper. Paragraph 2.2 expressly refers to the Computer Programs Directive<sup>35</sup> which prohibits the circumvention of technological devices applied to computer software. The Green Paper expressly states that “Community law does not require the introduction of technical systems for the protection of computer programs, but it does protect

---

<sup>27</sup> The Green Paper op cit note 17.

<sup>28</sup> <[http://europa.eu.int/documents/comm/index\\_en.htm](http://europa.eu.int/documents/comm/index_en.htm)> (visited on 11 March 2004).

<sup>29</sup> Clive Thorne ‘EC Green Paper on Copyright and Related Rights in the Information Society’ (1995) 54 *Copyright World* 14-23 at 14.

<sup>30</sup> SCADPlus *Green Paper on Copyright and Related Rights in the Information Society*, accessible at <<http://europa.eu.int?scadplus/leg/en/lvb/124152.htm>> (visited on 11 March 2004).

<sup>31</sup> Thorne op cit note 29 at 14.

<sup>32</sup> SCADPlus op cit note 30.

<sup>33</sup> Thorne op cit note 29 at 14.

<sup>34</sup> The EC Green Paper op cit note 17, para 1 at 79-82. Mihály Ficsor *The Law of Copyright and the Internet: The 1996 WIPO Treaties, Their Interpretation and Implementation* (2002) para 6.30 at 377.

<sup>35</sup> Article 7(1)(c) of the Council Directive 91/250/EEC of 14 May 1991 on the Legal Protection of Computer

those who install such systems by making it unlawful to put pirate decoding or other equipment into circulation or to possess it for commercial purposes.”

The Green Paper does not contain any suggestions as to how technological protection measures should be regulated. Paragraph 4 merely contains seven questions that will lay the groundwork for further preparatory work. Five of these seven questions deal with technological protection measures. Question 1 concerns the way in which technological protection measures may be established and operated in the countries of the European Community in relation to categories of works other than computer software. Question 3 relates to the legislative measures necessary and possible in respect of technological protection measures. Question 5 asks whether, in the event that these technological protection measures are introduced on a harmonized basis, the marketing and importation of any equipment not containing such protection measures should be proscribed. Question 6 raises the issue of whether international standards are necessary to ensure the effectiveness of technological protection measures. And Question 7 specifically invites comments on how it can be guaranteed that technological protection measures do not hinder access to data in the public domain.<sup>36</sup>

After the publication of the Green Paper interested parties lodged more than 350 submissions. The specific questions relating to the acquisition and management of rights<sup>37</sup> and the technical systems of identification and protection<sup>38</sup> were further discussed at a hearing in Brussels on 7 and 8 July 1994. The consultation process was concluded within the framework of a conference<sup>39</sup> organized by the Commission in Florence from 2 to 4 June 1996.<sup>40</sup>

### **5.2.2 The EC Proposal for the Protocol to the Berne Convention**

The language in the EC Proposal for the Protocol to the Berne Convention is nearly identical

---

Programs OJ L 122 , 17/05/1991 P 0042 – 0046 (the ‘Computer Programs Directive’).

<sup>36</sup> The Green Paper op cit note 17 at 83; Ficsor op cit note 34 para 6.30 at 377

<sup>37</sup> Section VIII, part 3, Chapter 2 of the Green Paper op cit note 17.

<sup>38</sup> Section IX, part 3, Chapter 2 of the Green Paper op cit note 17.

<sup>39</sup> *Copyright and Related Rights on the Threshold of the 21st Century*, organized by the European Commission, DG XV, in co-operation with the Italian Authorities, Florence, Italy, 2-4 June 1996.

<sup>40</sup> The Follow-Up Paper op cit note 19 para 2.

to that of the Clinton Administration's White Paper Bill.<sup>41</sup> The EC Proposal, like its US counterpart, contains a very broad prohibition on circumvention and circumvention devices:<sup>42</sup>

'Contracting Parties shall make unlawful, and provide for appropriate remedies against, the manufacture, distribution and possession for commercial purposes of any device, means or product, by any person knowing or having reasonable grounds to know that its primary purpose or effect is to remove, deactivate or circumvent, without authority, any process, mechanism or system which is designed to prevent or inhibit the infringement of any of the rights under the Berne Convention or this Protocol.'

### **5.2.3 The EC Follow-up Paper to the Green Paper on Copyright and Related Rights in the Information Society**<sup>43</sup>

On 20 November 1996, the Commission adopted a follow-up paper to the Green Paper. In 'Chapter 2: Priority issues for legislative action at Community level', the Commission identified priority issues. The focus was on the challenges that new technologies presented to copyright and related rights.<sup>44</sup> At this stage, the European Commission and the Member States were actively involved in preparing and negotiating the 1996 WIPO treaties, and the priority issues indicated in the follow-up paper also formed part of the WIPO treaties.<sup>45</sup>

Part 3 of Chapter 2, entitled 'Legal Protection of the Integrity of Technical Identification and Protection Schemes', addressed technological protection measures. It indicated that during consultations on the questions raised by the EC Green Paper, the majority of interested parties was in favour of adopting legislative measures to protect technological protection measures. The follow-up paper to the Green Paper<sup>46</sup> stated that '[a]n overwhelming majority of

---

<sup>41</sup> National Information Infrastructure Task Force, *Report of the Working Group on Intellectual Property and the National Information Infrastructure* (September 1995 (the 'US White Paper'); HR 2441, 10th Cong, 1st Sess (1995); S 1284, 104th Cong, 1st Sess (1995) (jointly referred to as the 'US White Paper Bill').

<sup>42</sup> The EC Proposal op cit note 18.

<sup>43</sup> The Follow-Up Paper op cit note 19.

<sup>44</sup> SCADPlus op cit note 30.

<sup>45</sup> Silke von Lewinski 'A Successful Step Towards Copyright and Related Rights in the Information Age: The New E.C. Proposal for a Harmonisation Directive' [1998] *European Intellectual Property Review* 135.

<sup>46</sup> Comments submitted in the consultation, Part 3, Chapter 2 of the Follow-Up Paper op cit note 19.

interested circles seeks the adoption of legislative measures providing for the legal protection of the integrity of technical identification and protection schemes'. However, the views varied on the exact scope of such legislative measures.

Only a minority favoured rules along the lines of article 7 of the Computer Programs Directive.<sup>47</sup> Article 7(1)(c) obliges Member States to provide appropriate remedies against any 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' (emphasis added). In terms of this provision, a device is prohibited only if its sole intended purpose is unauthorized circumvention. If a device has several purposes, only one of which is unauthorized circumvention, it is not prohibited.

The majority of interested parties, however, proposed broader protection than that provided for in article 7 of the Computer Programs Directive.<sup>48</sup> According to the follow-up paper to the Green Paper,

'[m]ost interested parties suggest, however, that legal protection should be more far reaching, covering also those products and services whose primary purpose or effect is to avoid, bypass, remove, de-activate or otherwise circumvent the copyright protection system. Others believe that the prohibited acts relating to the devices should also include use and import. They submit that these acts should not be restricted to those carried out for commercial purposes as such acts can cause extensive harm to rightholders.'<sup>49</sup>

The follow-up paper accordingly proposed that a standardized approach to interoperability amongst technological protection measures as well as the implementation of legal protection measures in relation to acts such as the circumvention, violation, or manipulation of these systems should be followed.<sup>50</sup> It suggests the following action:

---

<sup>47</sup> The Computer Programs Directive op cit note 35.

<sup>48</sup> Follow-Up Paper op cit note 19 at 16; Ficsor op cit note 34 at 378.

<sup>49</sup> Comments submitted in the consultation, Part 3, Chapter 2 of the Follow-Up Paper op cit note 19.

<sup>50</sup> Proposed action, Part 3, Chapter 2 of the Follow-Up Paper op cit note 19.

‘Any Commission proposal would have to precisely define the scope of protection and the nature of the appropriate sanctions. Due account will have to be taken of the principle of proportionality. This proposal would cover the properties of the protecting devices, the nature of the act to be covered (such as manufacture, possession in the course of business, putting into circulation, distribution, importation), the way or process of circumventing/ deactivating, etc. It should also ensure that systems are designed in a way which respects the right to privacy with regard to the processing of personal data.’<sup>51</sup>

It suggested, then, that not only the act of circumvention but also circumvention devices should be prohibited. The follow-up paper also identified the need to limit the prohibition:

‘In this context, the scope of the infringer’s liability has to be considered. This might possibly include legitimate defences to civil liability, and limitations to restricted acts and users’ rights have to be taken into account as well. In addition, appropriate civil penalties and/or sanctions may be called for.’<sup>52</sup>

#### **5.2.4 Proposal for a European Parliament and Council Directive on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society<sup>53</sup>**

Preparations for an EC Directive began in early 1997, immediately after the conclusion of the WIPO diplomatic conference<sup>54</sup> in 1996. On 10 December 1997, the European Commission presented a Proposal for a European Parliament and Council Directive on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society,<sup>55</sup> under the co-decision procedure of the European Parliament and the European Council of Ministers. The aim of the proposal was twofold – to implement the main objectives of the WCT, and to

---

<sup>51</sup> Proposed action, Part 3, Chapter 2 of the Follow-Up Paper op cit note 19.

<sup>52</sup> Ibid. Ficsor op cit note 34 para 6.3 at 378.

<sup>53</sup> The Proposal op cit note 20.

<sup>54</sup> Diplomatic Conference on Certain Copyright and Neighbouring Rights Questions in Geneva from 2 to 20 December 1996.

harmonize laws in the EU so as to ‘bring about a coherent and favourable environment for creativity and investment in the framework of the internal market’.<sup>56</sup>

In terms of clause 1.2, the proposed directive was to apply irrespective of existing directives,<sup>57</sup> unless such directives were expressly adapted.<sup>58</sup>

The proposal concentrated on rights and exceptions,<sup>59</sup> and on the protection of technological protection measures and rights management information.<sup>60</sup> Again, I shall focus on the protection of technological protection measures applied to works protected by copyright.

Clause 6 of the proposal deals with the protection of technological protection measures. It was believed that while ‘. . . technological development will allow rightholders to make use of technical measures designed to prevent and inhibit the infringement of any copyright. . .’, these technological measures could still be circumvented and copyright later infringed.<sup>61</sup>

Clause 6 was thus designed in response to the threat of circumvention.<sup>62</sup>

Clause 6 read as follows:

‘1. Member States shall provide adequate legal protection against any activities, including the manufacture or distribution of devices or the performance of services,

---

<sup>55</sup> The Proposal op cit note 20.

<sup>56</sup> Euan Lawson & Andre Steed ‘Sounds Unlimited 2: Music and Copyright in Cyberspace - An Update’ (1999) 90 *Copyright World* 16 at 17; SCADPlus op cit note 30.

<sup>57</sup> The Computer Programs Directive op cit note 35; Council Directive 92/100/EEC of November 19, 1992 on the Rental Right and Lending Right and on Certain Rights Related to Copyright in the Field of Intellectual Property, OJ EC L 346, at 61 (27 November 1992) (the ‘Rental Right Directive’); Council Directive 93/83/EEC of September 27, 1993, on the Co-ordination of Certain Rules Concerning Copyright and Rights Related to Copyright Applicable to Satellite Broadcasting and Cable Retransmission, OJ EC L 248, at 15 (6 October 1993); Council Directive 1993/98/EEC of October 29, 1993, Harmonizing the Term of Protection of Copyright and Certain Related Rights, OJ EC 290, at 9 (24 November 1993); European Parliament and Council Directive 96/9/EC of March 11, 1996, on the Legal Protection of Databases, OJ EC L 77, at 20 (27 March 1996) (the ‘Database Directive’).

<sup>58</sup> Article 10. See Lewinski op cit note 10 at 769.

<sup>59</sup> It is beyond the scope of this chapter to discuss whether users have a ‘right’ to demand access to and the making of non-infringing use of a copyright work. I have throughout this chapter used the words ‘exception’ and ‘limitation’ to signify what are otherwise also referred to as ‘exemptions’ to the exclusive rights held by authors. I will address this issue in Chapter 7.

<sup>60</sup> Reinbothe & Lewinski op cit note 4 at 202.

<sup>61</sup> Recital 30.

<sup>62</sup> See also Murray op cit note 16 at 192.

which have only limited commercially significant purpose or use other than circumvention, and which the person concerned carries out in the knowledge, or with reasonable grounds to know, that they will enable or facilitate without authority the circumvention of any effective technological measures designed to protect any copyright or any rights related to copyright as provided by law or the sui generis right provided for in Chapter III of European Parliament and Council Directive 96/9/EC.

‘2. The expression “technological measures”, as used in this Article, means any device, product or component incorporated into a process, device or product designed to prevent or inhibit the infringement of any copyright or any rights related to copyright as provided by law or the sui generis right provided for in Chapter III of Directive 96/9/EC. Technological measures shall only be deemed “effective” where the work or other subject matter is rendered accessible to the user only through application of an access code or process, including decryption, descrambling or other transformation of the work or other subject matter, with the authority of the rightholders.’

Clause 6 of the proposed directive sought to protect technological measures applied for the protection of not only copyright (as required by the WCT) and related rights (as required by the WIPO Performances and Phonograms Treaty (WPPT), but also for the sui generis right of database makers.<sup>63</sup> The EC thus goes beyond the provisions of the WCT and WPPT by providing similar protection for technological protection measures applied to databases. There is currently no international instrument requiring the legal protection of databases.<sup>64</sup>

Also in respect of the prohibited acts, the scope of the provisions of clause 6 were broader than those of the WCT – clause 6.1 sought to prohibit not only the act of circumvention but also the manufacture and distribution of devices, or the performance of services, that would enable or facilitate circumvention.<sup>65</sup>

---

<sup>63</sup> The Database Directive op cit note 57.

<sup>64</sup> Even though a proposal, entitled ‘Treaty on Intellectual Property in Respect of Databases’ was tabled for discussion at the Diplomatic Conference on Certain Copyright and Neighbouring Rights Questions in Geneva from 2 to 20 December 1996, it was never adopted.

<sup>65</sup> I shall refer to the latter prohibition as the prohibition on circumvention devices.

Clause 6.1 formulated a test to establish whether a device or service would be prohibited: it would be prohibited if it has ‘only limited commercially significant purpose or use other than circumvention’. This test was similar to the ‘commercially significant’ test formulated in *Sony Corp v Universal City Studios Inc.*<sup>66</sup> But while the *Sony* test is linked to copyright infringement, the clause 6.1 test was linked to circumvention. This meant that a device with limited commercially significant purpose or use other than circumvention would be prohibited, even if that circumvention was to facilitate entirely lawful acts.<sup>67</sup> However, the Explanatory Memorandum to the Proposal stated that ‘not any circumvention of technical means of protection should be covered, but only those which constitute an infringement of a right, i.e. which are not authorised by law or by the author’.<sup>68</sup> The clause 6.1 test also differed from the ‘sole intended purpose’ test of article 7.1(c) of the Computer Programs Directive. So the test to determine whether a circumvention device was prohibited depended on whether the technological protection measure protected software or whether it protected any other category of copyright works.

Clause 6.1 had an objective and a subjective requirement.

It subjectively required ‘knowledge’ or ‘reasonable grounds to know’ on the part of the circumventor. Unfortunately, clause 6.1 linked this knowledge requirement to circumvention, and not to infringement.

Clause 6.1 also required the circumventor to know that the device would enable or facilitate circumvention ‘without authority’. This was an objective requirement. But it was unclear whether this ‘without authority’ criterion applied to the act of circumvention itself, or to the act facilitated by the circumvention (such as the reproduction or translation of the work).<sup>69</sup> If

---

<sup>66</sup> 464 US 417 (1984).

<sup>67</sup> Thomas Vinje ‘Copyright Imperilled?’ [1999] *European Intellectual Property Review* 192 at 206.

<sup>68</sup> Explanatory Memorandum, The Proposal op cit note 20 referred to by Michael Hart ‘The Proposed Directive for Copyright in the Information Society: Nice Rights, Shame about the Exceptions’ [1998] *European Intellectual Property Review* 169 at 171.

<sup>69</sup> Article 11 of the WCT expressly states that the only technological protection measures that are protected are those ‘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’ (emphasis added). Article 11 therefore expressly links authority to subsequent infringement,

it applied to the act of circumvention itself, it would have been meaningless. It was also unclear whether the term ‘authority’<sup>70</sup> included legal permissibility (such as the exceptions provided by copyright legislation), or whether it was limited to permission granted by the author. According to Casellati,<sup>70</sup> the words ‘without authority . . . as provided by law’ allowed circumvention in order to benefit from copyright exceptions. It seems as if this was indeed the intention of the Commission: in the light of the statement in its Explanatory Memorandum,<sup>71</sup> its proposal apparently should be read to prohibit only circumvention where the act facilitated by circumvention infringes copyright. So it seems that the phrase ‘without authority’ was linked to subsequent copyright infringement, and that the term ‘authority’ included not only permission granted by the author but also ‘authority’ granted by law.<sup>72</sup>

Clause 6.2 defined a technical measure as ‘. . . any device, product or component incorporated into a process, device or product designed to prevent or inhibit the infringement of any copyright or related rights related to copyright as provided by law or. . .’ the Database Directive.<sup>73</sup> Only ‘effective’ technological protection measures were protected. It is interesting to note here that clause 6.2 expressly stated that a measure would be deemed effective ‘where the work or other subject matter is rendered *accessible* to the user. . .’ (emphasis added). So effectiveness is linked to access rather than infringement. According to Koelman,<sup>74</sup> this means that only measures that would have controlled access were covered by the provisions. Also, if the prohibition was interpreted to connote that only technological protection measures that prevented copyright infringement<sup>75</sup> would be covered, it would have had the effect that not many technological protection measures would have been protected against circumvention. Systems that only control copying would not have been covered, since they do not control unauthorized access to a work. The same applied to systems that

---

and not to the act of circumvention itself.

<sup>70</sup> Casellati op cit note 22 at 374-375.

<sup>71</sup> The Explanatory Memorandum, the Proposal op cit note 20 states that “not any circumvention of technical means of protection should be covered, but only those which constitute an infringement of a right, i.e. which are not authorized by law or by the author”.

<sup>72</sup> Casellati op cit note 22 at 375; Vinje op cit note 67 at 206.

<sup>73</sup> Murray op cit note 16 at 192.

<sup>74</sup> Kamiel J Koelman ‘A Hard Nut to Crack: The Protection of Technological Measures’ [2000] *European Intellectual Property Review* 272 at 275.

<sup>75</sup> See Recital 30: ‘legal protection should be provided to technological measures that *effectively inhibit and/or prevent* the infringement of any copyright...’ (emphasis added)

controlled unauthorized access, as since access was not an exclusive right of a author.<sup>76</sup>

Several objections were raised against clause 6. One objection was against the ‘commercially significant’ test proposed to be used to determine whether a circumvention device was prohibited. The music industry argued that this would mean that copyright pirates could simply add commercially significant purposes to their circumvention devices in order to make them legitimate.<sup>77</sup> It was also argued that a wide range of technologies, especially in the record industry, already existed that had several purposes, some of them commercially significant. Despite these commercially significant uses, these technologies could also be used to circumvent protection measures. If the ‘commercially significant’ test were to be used, these technologies would not have been prohibited.<sup>78</sup> One suggestion was for the wording of clause 6.1 to be improved to clarify that the devices and services included those that had the sole purpose of circumvention.<sup>79</sup>

There were also calls for clause 6 to make it unlawful to circumvent technological protection measures even for the purpose of doing something lawful, on the ground that it might be impossible to tell whether an act or device was intended to circumvent for a lawful or unlawful reason. However, such a prohibition could lead to a technical monopoly of copyright works extending far beyond the limits of traditional copyright protection.<sup>80</sup>

Clause 6 did not contain any specific exceptions. It was also not subject to the exceptions contained in clause 5 – the heading of clause 5 expressly referred only to clauses 2 and 3 (dealing with the reproduction right and the public communication right, respectively). The Explanatory Memorandum to clause 5<sup>81</sup> expressly states that this provision harmonizes the restrictions and limitations ‘with respect to the reproduction right and the right of communication to the public’.<sup>82</sup> It does not refer to the prohibition on circumvention. So clause 6 seemingly proposed to create an unlimited right for authors. However, as explained

---

<sup>76</sup> Koelman op cit note 74 at 275.

<sup>77</sup> Hart op cit note 68 at 171.

<sup>78</sup> Lawson & Steed op cit note 56 at 18.

<sup>79</sup> Lewinski op cit note 45 at 138n16.

<sup>80</sup> Hart op cit note 68 at 171.

<sup>81</sup> Point 1.

<sup>82</sup> Lewinski op cit note 10 at 775.

above, it seems as if the objective ‘without authority’ requirement also included copyright exceptions: although clause 6 was not expressly made subject to clause 5, it still would have been subject to existing copyright exceptions.<sup>83</sup>

Approximately 300 objections were received on the original proposal. The European Commission consequently amended its proposal.<sup>84</sup>

### **5.2.5 Amended proposal for a European Parliament and Council Directive on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society<sup>85</sup>**

On 20 January 1999, the Legal Affairs Committee of the European Parliament adopted a report by Roberto Barzanti on the views of the European Commission on the proposed directive.<sup>86</sup> The Committee tried, among other things, to clarify the wording of clause 6.<sup>87</sup> The Barzanti amendments took the form of additions to the original proposal (as opposed to wholesale deletions and replacements).<sup>88</sup> The European Parliament adopted its report on the proposal in February 1999,<sup>89</sup> and the European Commission presented its Amended Proposal on 21 May 1999.<sup>90</sup>

Clause 6 of the Amended Proposal provided as follows:

‘1. Member States shall provide adequate legal protection against the circumvention without authority of any effective technological measures designed to protect any copyright or any rights related to copyright as provided by law or the *sui generis* right provided in Chapter III of the European Parliament and Council Directive 96/9/EC,

---

<sup>83</sup> The Explanatory Memorandum to the Proposal op cit note 20 states that ‘not any circumvention of technical means of protection should be covered, but only those which constitute an infringement of a right, i.e. which are not authorised by law or by the author’. See also Casellati op cit note 22 at 374.

<sup>84</sup> MT Michéle Rennie ‘E.U. Copyright Directive: May 1999 Amendments to Appease Some Industry Sectors’ (1999) 5 *Computer and Telecommunications Law Review* 123.

<sup>85</sup> The Amended Proposal op cit note 21.

<sup>86</sup> Lawson & Steed op cit note 56 at 18.

<sup>87</sup> Ibid.

<sup>88</sup> Idem at 18-19.

<sup>89</sup> Opinion of the European Parliament of 10 February 1999 [1999] OJ C150/171.

<sup>90</sup> The Amended Proposal op cit note 21.

which the person concerned carries out in the knowledge, or with reasonable grounds to know that he or she pursues that objective.

‘2. Member States shall provide adequate legal protection against any activities, including the manufacture or distribution of devices, products or components or the provision of services carried out without authority, which:

- (a) are promoted, advertised or marketed for the purpose of circumvention, or
- (b) have only a limited commercial significant purpose or use other than to circumvent, or
- (c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of,

any effective technological measures designed to protect any copyright or any right related to copyright as provided by law or the *sui generis* right provided for in Chapter of European Parliament and Council Directive 96/9/EC.

‘3. The expression “technological measures” as used in this Article means any technology, device or component that in the normal course of its operation, is designed to prevent or inhibit the infringement of any copyright or related rights related to copyright as provided by law or the *sui generis* right provided for in Chapter III of European Parliament and Council Directive 96/9/EC.

‘Technological measures shall be deemed “effective” where the access to or use of a protected work or other subject matter is controlled through application of an access code or any other type of protection process which achieves the protection objective in an operational and reliable manner with the authority of the rightholders. Such measures may include decryption, descrambling or other transformation of the work or subject matter.’

Clause 6.1 of the Amended Proposal expressly required that the technological measure be ‘designed’ to protect copyright. According to Koelman,<sup>91</sup> this implied that the measure would be protected as long as it was initially designed to prevent copyright infringement, regardless

of whether, under the circumstances, it actually protected copyright.

Clause 6.1 also required that the circumvention had to take place ‘without authority’ in order to be prohibited. From comment 3 in respect of clause 6 in the Explanatory Memorandum it can be understood that this requirement was meant to express that there might be cases where an exception ‘authorizes’ circumvention. However, copyright exceptions do not authorize any acts of circumvention. So clause 6 did not provide a clear link between the scope of protection of technological protection measures and the scope of copyright. In the wording of article 11 of the WCT, the acts subsequent to circumvention that may be ‘authorized’ by law, not the act of circumvention itself. So although in the wording of the WCT the copyright limitations affect the extent to which technological protection measures have to be protected, this was not the case with the Amended Proposal.<sup>92</sup>

Clause 6.1 again included a subjective requirement (the objective requirement being ‘without authority . . . as provided by law’). While the Proposal expressly linked knowledge to circumvention, the Amended Proposal linked knowledge to ‘that objective’. What objective, though? The objective of copyright infringement, or the objective of circumvention? Casellati<sup>93</sup> believes it referred to the objective of copyright infringement. If, like in the Proposal, the knowledge requirement were to apply to the act of circumvention, a person would have been liable if she circumvented technological protection measures, even if she did not know that the protected work was a copyright work.

Clause 6.2 required Member States to provide adequate control of products or services that had as their primary or only aim the circumvention of technological protection devices. Clause 6.2 proposed to replace the ‘commercially significant’ test for circumvention devices with three alternative tests fashioned after the DMCA. It also provided, like its counterpart in the DMCA, that this test could be applied to parts or components of a device or service, and not just to the device or service as a whole. Hence, a service or device that fell into any of the following categories was prohibited:<sup>94</sup> (a) a device or service that was promoted, advertised,

---

<sup>91</sup> Koelman op cit note 74 at 273.

<sup>92</sup> Idem.

<sup>93</sup> Casellati op cit note 22 at 375.

<sup>94</sup> Dean S Marks & Bruce H Turnbull ‘Technical Protection Measures: The Intersection of Technology, Law

or marketed for the purpose of the circumvention any effective technological measure designed to protect any copyright;<sup>95</sup> (b) a device or service that had only a limited commercial significant purpose or use other than to circumvent any effective technological measure designed to protect any copyright,<sup>96</sup> and (c) a device or service that was primarily designed, produced, adapted, or performed for the purpose of enabling or facilitating the circumvention of any effective technological measure designed to protect any copyright.<sup>97</sup>

The actual protection extended to authors against these devices or services and the enforcement of the protection were proposed to be left to individual Member States. They were given much freedom as to how they would implement clause 6.<sup>98</sup> This would have allowed for a significant degree of variation within the EC.

The ‘carried out with authority’ requirement may have been intended to indicate that these activities would be lawful if they were authorized by copyright law – if the activities were covered by copyright exceptions and limitations. But the provision did not clarify that devices were permissible if they were primarily produced, marketed, or designed for the purpose of lawful circumvention. Rather, it covered circumvention devices that enabled circumvention, generally.<sup>99</sup>

Also, clause 6.2 still allowed the possibility of lawful devices being caught by clause 6.2(b). Kennedy<sup>100</sup> gives the example of a device initially developed for a lawful purpose but which for some reason proves unpopular. If this same device is later put to a much more popular use to circumvent technological protection measures, it will be caught by clause 6.2(b).

Unlike its United States counterpart, clause 6.3 of the Amended Proposal did not distinguish

---

and Commercial Licences’ [2000] *European Intellectual Property Review* 198 at 201.

<sup>95</sup> Corresponding to 17 USC § 1201(a)(2)(C) and (b)(1)(C).

<sup>96</sup> Corresponding to 17 USC § 1201(a)(2)(B) and (b)(1)(B).

<sup>97</sup> Corresponding to 17 USC § 1201(a)(2)(A) and (b)(1)(A).

<sup>98</sup> This is in contrast to the express statement in the Follow-Up on the Green Paper that a standardized approach to the implementation of legal protection measures in relation to acts such as circumvention should be followed. See also Michael Doherty & Ivor Griffiths ‘The Harmonisation of European Union Copyright Law for the Digital Age’ [2000] *European Intellectual Property Review* 17 at 19.

<sup>99</sup> Koelman op cit note 74 at 274.

<sup>100</sup> Gabriela Kennedy ‘Copyright in the Information Society: A World of More Copies and Rights’ (1999) 93 *Copyright World* 15 at 19.

between measures controlling access and measures protecting copyright – it merely referred to measures protecting copyright and any right related to copyright as provided by law. But one of the requirements that a technological protection measure should meet before it will be protected is that it should be effective. In terms of clause 6.3, a measure would be deemed to be effective ‘where the *access to or use of* a protected work . . . is controlled through application of . . .’ a technological measure (emphasis added). A measure controlling ‘access to’ a protected measure is an access control, whereas a measure controlling ‘use of’ a work is a copy control. In sharp contrast to the Proposal, which covered only access control, the Amended Proposal covered both access and copy control. Also, by expressly including access control in the definition of ‘effectiveness’ it seems as if the intention of the framers of the Proposal and the Amended Proposal was to broaden the scope of copyright to include an access right, otherwise it would have been sufficient for the definition to refer copy control measures.<sup>101</sup>

Clause 6 of the Amended Proposal, like its predecessor in the Proposal, contained no express exceptions to the prohibition on the circumvention of technological protection measures. Clause 5, dealing with exceptions, expressly limited the exceptions contained in it to the restricted acts set out in clauses 2, 3, and 4.

What is interesting to note, however, is that clause 5.2(b)bis of the Amended Proposal implied that exceptions allowing private copying could be abolished if technological protection measures enabled authors to control such copying. Recital 27 added that these ‘exceptions should not inhibit the use of technological measures or their enforcement against circumvention’. Apparently, then, at least the private copying exceptions in national copyright laws did not affect the protection of technological protection measures. The European Parliament proposed to insert a sentence into clause 5.4 stating that none of the exceptions contained in article 5 would block the protection of technological protection measures.<sup>102</sup> The Commission decided not to incorporate this suggestion in the Amended

---

<sup>101</sup> Koelman op cit note 74 at 275.

<sup>102</sup> European Parliament, minutes of 10 February 1999, A4-0026/99, cited by Koelman op cit note 74 at 274. The text of the amendment was: ‘these exceptions and limitations must not prevent the use of technical means to protect works with the aim of safeguarding the interests of the rightholders, nor prejudice the protection of these means as referred to in Article 6.’

Proposal. Koelman<sup>103</sup> believes that one could conclude, from this refusal, that the Commission intended that all copyright exceptions, apart from those concerning private copying, would affect the protection of technological protection measures.

Clause 8 sought to oblige Member States to provide appropriate sanctions and remedies for a violation of the rights and obligations set out in the instrument. It did not specify that these sanctions and remedies should include civil and criminal sanctions and remedies. It merely referred to ‘sanctions’ and ‘remedies’.<sup>104</sup> It is uncertain whether this proposal would have required the availability of civil remedies when the prohibition in clause 6 was violated. Even though clause 8 may have required the availability of certain civil remedies to ‘rightholders whose interests are affected by an infringing activity’, if one assumes that neither circumvention nor the trafficking in circumvention devices is a copyright infringing act, granting authors the right to sue for damages and to apply for injunctions and seizure would not have been necessary. This is also Koelman’s conclusion.<sup>105</sup> But he also states, with reference to comment 2 on clause 8 in the Explanatory Memorandum, that a contrary conclusion may well be appropriate, as the reasoning in the Memorandum was perhaps the result of a misconception of circumvention and trafficking in circumvention devices as constituting copyright infringing acts. Member States then could, if Koelman were correct, implement clause 6 in criminal law and leave the decision to prosecute to public authorities.

It was once again proposed that it be left to each individual Member State to provide for the enforcement of these rights and obligations.<sup>106</sup> Kennedy<sup>107</sup> recognizes as one of the shortcomings of the Amended Proposal the fact that there is no consistent approach regarding the enforcement of rights throughout the EC. The Amended Proposal specified at length the rights, their protection, and exceptions, but the absence of infringement provisions in the Amended Proposal meant that when it came to enforcement, authors would have had to do a fair amount of homework to ensure that the jurisdiction that offered the desired remedies was

---

<sup>103</sup> Koelman op cit note 74 at 274.

<sup>104</sup> Article 8.1.

<sup>105</sup> Koelman op cit note 74 at 277 and also note 44 at 277.

<sup>106</sup> Article 8.2.

<sup>107</sup> Kennedy op cit note 100 at 18.

selected. So the Amended Proposal seems to encourage a fair amount of forum shopping.<sup>108</sup>

The Amended Proposal sought to dispel the worry that the protection of technological measures would create a monopoly in the hands of authors. Recital 10bis stated that technological measures to protect works were essential to give effect to the principles and guarantees laid down by the law, whereas recital 30bis, in turn, stated that no obligation was imposed on authors to utilize such measures.<sup>109</sup>

The main criticism against the Amended Proposal was that its provisions were one-sided in that they denied rights to many. Especially access to material would have been difficult to obtain. The main suggestions to address this criticism were more extensive exceptions to the provisions, and different methods of dealing with access issues.<sup>110</sup>

A further point of criticism was that it seemed that the proposed Directive would not yield much by way of harmonization because of the extent of the autonomy granted to Member States.<sup>111</sup>

## **5.3 The Copyright Directive**

### **5.3.1 Background**

On 16 March 2000, the 'Internal Market' Council of Ministers approved, on behalf of the EC, the two WIPO treaties without discussion.<sup>112</sup>

The instrument of ratification was deposited on behalf of the EC in accordance with the principle that the European Commission represents the entire Community and its member states abroad.<sup>113</sup>

---

<sup>108</sup> Ibid.

<sup>109</sup> Idem at 19.

<sup>110</sup> Doherty & Griffiths op cit note 98 at 18 and 20.

<sup>111</sup> Idem at 18.

<sup>112</sup> OJ L89/6 11/4/2000 accessible at

<[http://europa.eu.int/comm/internal\\_market/en/intprop/news/ratification.htm](http://europa.eu.int/comm/internal_market/en/intprop/news/ratification.htm)> (visited on 5 May 2002).

<sup>113</sup> <[http://europa.eu.int/comm/internal\\_market/en/intprop/news/ratification.htm](http://europa.eu.int/comm/internal_market/en/intprop/news/ratification.htm)> (visited on 5 April 2002).

The Council agreed on the common position of the Amended Proposal in September 2000, and the European Commission accepted the common position without changes on 20 October 2000.<sup>114</sup> Subsequent to the second reading in the European Parliament in February 2001,<sup>115</sup> the Copyright Directive was adopted on 22 May 2001. It came into force on 22 June 2001.<sup>116</sup> The Directive had to be implemented by the Member States by 22 December 2002.<sup>117</sup> This deadline was not met.<sup>118</sup>

The Copyright Directive has two principal aims – to implement the WIPO treaties, and to bring greater harmonization to European copyright law.<sup>119</sup>

### 5.3.2 Technological Protection Measures

Article 6 of the Copyright Directive implements article 11 of the WCT. It seeks to protect ‘effective technological measures’. Like the corresponding provision in the Proposal, article 6 is far more ambitious than article 11 of the WCT in that it seeks to add operational substance to article 11 of the WCT. Although many objections can be raised against such detailed provisions, Reinbothe and Lewinski<sup>120</sup> are of the opinion that it was necessary to make the protection of technological protection measures provided for under the WCT operational.

Article 6.1 prohibits acts of circumvention, article 6.2 prohibits circumvention devices (also referred to as ‘preparatory acts’),<sup>121</sup> and article 6.3 defines the term ‘technological measure’. Article 6.4 then qualifies the protection against acts of circumvention under article 6.1 with reference to certain exceptions and limitations.

---

<sup>114</sup> <<http://eurorights.org/eudmca/>> (visited on 20 March 2002).

<sup>115</sup> Council Common Position on 28 September 2000 [2000] OJ C344/1.

<sup>116</sup> The Copyright Directive op cit note 6.

<sup>117</sup> Reinbothe & Lewinski op cit note 4 at 203.

<sup>118</sup> At date of writing, five member states still had to adopt the Directive.

<sup>119</sup> Michael Hart ‘The Copyright in the Information Society Directive: An Overview’ [2002] *European Intellectual Property Review* 58.

<sup>120</sup> Reinbothe & Lewinski op cit note 4 at 204.

<sup>121</sup> Jörg Reinbothe & Silke von Lewinski *The WIPO Treaties 1996* (2002) \*\*\*n23; Reinbothe & Lewinski op cit note 4 at 204n38.

Article 6.3 defines a ‘technological measure’ as ‘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 authorized by the right holder of any copyright or any right related to copyright as provided for by law or the *sui generis* rights provided for in Chapter III of Directive 96/9/EC’.

In terms of this definition, then, a ‘technological measure’ is a measure that prevents or restricts acts ‘not authorized by the right holder of any copyright or any right related to copyright as provided for by law’. Since access is not one of the author’s exclusive rights, it seems at first blush as if only copy controls are covered by this definition. However, article 6 protects not mere ‘technological measures’ – they have to be ‘effective’. Article 6.3 continues that a technological measure is deemed to be ‘effective’ where ‘[t]he use of a protected work or other subject-matter is controlled by [authors] through 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’ (emphasis added). So the reference to ‘effective technological measures’ in article 6 includes access and copy control (‘protection process’).<sup>122</sup>

Article 6.3 requires that the measure should achieve its ‘protection objective’ in order to be effective. This does not mean that the technological measure has to be infallible. The phrase ‘in the normal course of its operation’ should also be considered in the context of ‘effectiveness’. As this phrase is synonymous with the phrase ‘in the ordinary course of its operation’ in the DMCA, the Copyright Directive may well work with the same concept of ‘effectiveness’ as its United States counterpart.<sup>123</sup>

It seems, though, as if the definition is circular, which, according to Lipton,<sup>124</sup> can undermine its usefulness. According to article 6.3 a measure is ‘effective’ if it ‘achieves the protection objective’. Arguably, if a measure achieves its intended protection objective, there is no need for the law to protect it.

---

<sup>122</sup> See also the comments on the Amended Proposal by Koelman op cit note 74 at 275.

<sup>123</sup> Ficsor op cit note 34 at 546.

<sup>124</sup> Lipton op cit note 2 at 346.

Another interpretation of the meaning of ‘effectiveness’ is advanced by Koelman and Helberger:<sup>125</sup> a measure is ‘effective’ only as long as it is not accidentally circumvented. A person circumventing an ‘effective’ technological measure at least knows that she is dealing with a protection measure.

Caselatti<sup>126</sup> disagrees:

‘[T]he effectiveness requirement is not related to the effectiveness of rightholders’ protection in general, but has to be attached to the particular function carried out by that specific measure. This leads us to the conclusion that not every accidental circumvention of a [technological protection measure] makes that measure “ineffective”.’

She believes that the determining factor for effectiveness is the technological capabilities of the measure rather than how useful it is to authors. If she is correct, there will be very few ‘effective’ technological protection measures.

Article 6.3 states that the term ‘technological measure’ connotes any measure designed to prevent or restrict ‘acts . . . which are not authorized by the rightholder of any copyright or a right related to copyright as provided for by law’. Thus, the circumvention of technological measures protecting against acts authorized by the author or the holder of a related right (a ‘neighbouring right’ in older copyright terminology) is not prohibited. Related rights are, for example, performers’ rights, and so the reference in article 6.3 to a ‘right related to copyright as provided for by law’ should not be read to refer to fair use and reverse engineering, for example. What is clear, though, is that the lawfulness criterion attaches to the technological measure and not to the act of circumvention. Von Coppenhagen<sup>127</sup> believes that it should rather have been the other way round.

---

<sup>125</sup> Kamiel Koelman & Natali Helberger ‘Protection of Technological Measures’ *IMPRIMATUR* (Nov 1998) at 19 accessible at <<http://www.imprimatur.net/download.htm>> cited by Casellati op cit note 22 at 376.

<sup>126</sup> Casellati op cit note 22 at 396-397.

<sup>127</sup> Vanessa van Coppenhagen ‘Copyright and the WIPO Copyright Treaty, with Specific Reference to the Rights Applicable in a Digital Environment and the Protection of Technological Measures’ (2002) 119 *South*

I shall first discuss the prohibition on the act of circumvention, then the prohibition on circumvention devices, and finally the related exceptions and limitations.

### 5.3.3 The Prohibition

#### 5.3.3.1 The Prohibition on Conduct

Article 6.1 of the Copyright Directive obliges Member States to

‘provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.’<sup>128</sup>

Article 6.1 is mandatory – it obliges Member States to provide legal protection against the *act* of circumvention. The prohibition is not limited to acts of circumvention for purposes of copyright infringement.<sup>129</sup>

The phrase ‘without authority’ which appeared in the Proposal and Amended Proposal is eliminated from the final wording of the article 6.1. As I explained above, the term ‘authority’ referred to copyright exceptions and limitations. So to reintroduce the concept ‘authority’ and in this way to legitimize circumvention for non-infringing purposes, a new article 6.4 was added. This provision now addresses the relationship between technological protection measures and copyright exceptions and limitations.<sup>130</sup> But more about this below.

The subjective ‘knowledge’ requirement remained part of article 6.1. According to Casellati,<sup>131</sup> it seems as if this requirement lost the importance it had for exceptions and limitations in the earlier versions of the text, as exceptions and limitations are now addressed

---

*African Law Journal* 429 at 444.

<sup>128</sup> Hart op cit note 119 at 62.

<sup>129</sup> Charlotte Waelde ‘The Quest for Access in the Digital Era: Copyright and the Internet’ (2001) 1 *The Journal of Information, Law and Technology* at 7 accessible at <<http://elj.warwick.ac.uk/jilt/01-1/waelde.html>>.

<sup>130</sup> Casellati op cit note 22 at 376.

separately. One view is that the knowledge requirement makes sense only when the circumvention occurs accidentally. But others argue that a technological measure is ‘effective’ only so long as it is not accidentally circumvented.<sup>132</sup> If this argument is correct, the knowledge requirement is clearly redundant.

From the wording of the text it seems that the knowledge requirement is now linked to circumvention, not to infringement. It seems as if the person circumventing should carry out the circumvention in the knowledge that she is pursuing the objective of circumvention, not the objective of copyright infringement.

It is interesting to note that the Computer Programs Directive,<sup>133</sup> dealing with the circumvention of technological measures protecting computer programs (a category of copyright works), does not contain a corresponding prohibition on the act of circumvention.<sup>134</sup> The act of circumventing a technological measure applied to computer programs is not prohibited. Neither does the Conditional Access Directive<sup>135</sup> prohibit the act of circumvention. It targets only the commercial dealing in devices that enable unauthorized circumvention. The thinking behind leaving private non-commercial activities outside the ambit of the Conditional Access Directive is that the enforcement of provisions aimed at private behaviour would conflict with the right to privacy, and would be impossible to enforce.<sup>136</sup> Why does the Copyright Directive target the act of circumvention? Is user privacy less likely to be violated while enforcing a provision aiming at the circumvention of

---

<sup>131</sup> Ibid.

<sup>132</sup> See, for example, Kamiel Koelmann & Natali Helberger ‘Protection of Technological Measures’ IMPRIMATUR (Nov 1998 at 19, available at <<http://www.imprimatur.net/download.htm>>, cited by Casellati op cit note 22 at 376.

<sup>133</sup> The Computer Programs Directive op cit note 35.

<sup>134</sup> The Computer Programs Directive does not directly prohibit ‘computer crimes’, that is, unauthorized access to a computer itself. It only forbids possession or circulation of items designed to remove or bypass technical devices protecting a computer program, which should help to safeguard password-protected upload systems as well as access or copy protected software content distributed on the network (Allen N Dixon & Laurie C Self ‘Copyright Protection for the Information Superhighway’ [1994] *European Intellectual Property Review* 465 at 468.

<sup>135</sup> Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the Legal Protection of Services Based on, and Consisting of, Conditional Access (the ‘Conditional Access Directive’).

<sup>136</sup> Council of Europe, Recommendation R(91)14, The Legal Protection of Encrypted Television Services, September 27, 1991. The commentary on article 3 in the Explanatory Memorandum with the Conditional Access Directive refers to this recommendation (cited by Koelman op cit note 74 at 277n41).

technological protection measures that protect copyright?<sup>137</sup>

Article 6.1, then, prohibits the act of circumventing access and copy control. Its counterpart in the DMCA merely prohibited the act of circumventing access control.

### 5.3.3.2 The Prohibition on Devices

The prohibition on circumvention devices is not new in European law. In June 1988, the European Commission published its *Green Paper on Copyright and the Challenges of Technology – Copyright Issues Requiring Immediate Action*.<sup>138</sup> Chapter 3 dealt with the problem of Digital Audio Tape (DAT) machines. One of the conclusions was that the manufacture, importation, or sale of devices intended to circumvent copy protection should be prohibited.<sup>139</sup>

The first Directive covering technological measures was the Conditional Access Directive.<sup>140</sup> This Directive is aimed at protecting radio and television broadcasting services and ‘information society services’ (such as video on demand, on-line information services, and electronic newspapers) that are provided against remuneration and on the basis of conditional access.<sup>141</sup> It prohibits trafficking in ‘illicit devices’,<sup>142</sup> and defines an ‘illicit device’ as ‘any equipment or software designed or adapted to give access to a protected service in an intelligible form without the authorization of the service provider’.

The Conditional Access Directive protects only against unauthorized access to a protected *service*, and not against unauthorized access to a *copyright work*.<sup>143</sup>

---

<sup>137</sup> Koelman op cit note 74 at 277.

<sup>138</sup> Ficsor op cit note 34 at 364.

<sup>139</sup> Idem at 365.

<sup>140</sup> The Conditional Access Directive op cit note 135.

<sup>141</sup> Article 2(a) and (b).

<sup>142</sup> Article 4 of the Conditional Access Directive provides that:

‘Member States shall prohibit on their territory all of the following activities:

- (a) the manufacture, import, distribution, sale, rental or possession for commercial purposes of illicit devices;
- (b) the installation, maintenance or replacement for commercial purposes of an illicit device;
- (c) the use of commercial communications to promote illicit devices.’

<sup>143</sup> According to the Commission, the Conditional Access and Copyright Directives are complementary. It seems

Article 6.2 of the Copyright Directive states the following:

‘Member States shall 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,
  - (b) have only a limited commercially significant purpose or use other than to circumvent, or
  - (c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of,
- any effective technological measures.’

Article 6.2, like article 6.1, is mandatory. It prohibits the trafficking in circumvention devices for commercial purposes. It 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’ circumvention devices (emphasis added). There is some debate about the import of ‘commercial purposes’ in article 6.4. Was it really intended to exempt non-commercial infringement?<sup>144</sup> I believe that this implies that where a device is manufactured exclusively to perform an exempted act of circumvention, and not for commercial purposes, such device is exempted. This means that, unlike its counterpart in the DMCA, article 6.2 does not prohibit the means with which to perform legitimate acts of circumvention.

Article 6.2 contains three alternative tests to determine whether a particular device is regarded as a circumvention device. These three tests correspond to those in the Proposal and

---

appropriate to distinguish between unauthorized access to a remunerated service and unauthorized exploitation of works protected by copyright. Although there are basic differences between the technological measures provisions in the Access Directive and in the Copyright Directive, the protection offered by the two directives might, according to Vinje, often practically coincide, because a technological measure that prevents unauthorised access to a service will in many instances also effectively protect the copyright content of the service (Vinje op cit note 67 at 205-206).

<sup>144</sup> Nick Hanbidge ‘Protecting Rights Holders’ Interests in the Information Society: Anti-circumvention; Threats

the DMCA. Article 6.2 also provides, like its counterparts in the DMCA and the Amended Proposal, that these tests may be applied to parts or components of a device or service, and not just to the device or service as a whole.

Although computer programs are also subject to copyright, they are regulated by the Computer Programs Directive<sup>145</sup> and not by the Copyright Directive.<sup>146</sup> This means that article 6 of the latter Directive applies to all categories of copyright works except computer programs. Although article 7.1(c) of the Computer Programs Directive<sup>147</sup> corresponds to article 6.2 of the Copyright Directive, the Computer Programs Directive contains only one test to determine whether a device is a circumvention device. Article 7.1(c) outlaws 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. Thus, if a device has a dual purpose, one lawful and the other unlawful, it is not regarded as a circumvention device and so is not prohibited. By contrast, paragraphs (b) and (c) of article 6.2 of the Copyright Directive refer to devices that have only a *limited commercially significant purpose* or use other than to circumvent, or which are *primarily designed* to enable or facilitate such circumvention.<sup>148</sup> Under this Directive, a dual purpose device, even where one purpose is lawful, is prohibited as a circumvention device.

Article 7.1(c) of the Computer Programs Directive targets only the *trade* in circumvention devices. This Directive does not make the use of a circumvention device to circumvent a protective measure unlawful. The Copyright Directive, by contrast, targets the act of circumvention, and so makes the use of circumvention devices unlawful.<sup>149</sup>

Although computer programs are also a category of copyright works, the circumvention of technological protection measures applied to such works are subject to a set of rules different from the circumvention of technological protection measures applied to any other category of

---

Post-Napster; and DRM' (2001) 12 *Entertainment Law Review* 223.

<sup>145</sup> The Computer Programs Directive op cit note 35

<sup>146</sup> Hart op cit note 119 at 62.

<sup>147</sup> The Computer Programs Directive op cit note 35.

<sup>148</sup> Hart op cit note 119 at 62.

copyright works.

### **5.3.4 The Responsibility of Equipment Manufacturers**

The text of the Copyright Directive does not expressly contain a ‘no-mandate’ provision like the DMCA.<sup>150</sup> However, recital 48 states that ‘[s]uch 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’.<sup>151</sup>

### **5.3.5 The Obligations of Authors**

In one important respect the Copyright Directive differs from the DMCA: article 6.4 of the Copyright Directive requires Member States to take appropriate measures to ensure that users have the means to benefit from certain specified exceptions or limitations, provided that the beneficiary has legal access to the protected works.

Authors who use technological protection measures can either conclude voluntary agreements concerning the manner in which the means for benefiting from exceptions or limitations will be made available to users with valid access, or Member States will oblige them to make such means available.

### **5.3.6 Limiting the Application of Article 6**

The application of the prohibition in Article 6 is limited in three ways. In the first instance, the Directive provides for a monitoring system. Secondly, the Directive contains a savings clause. And, thirdly, the Directive provides for specific exceptions to the prohibition on circumvention.

---

<sup>149</sup> Koelman op cit note 74 at 272.

<sup>150</sup> 17 USC § 1201(c)(3).

<sup>151</sup> Ficsor op cit note 34 para 11.20 at 554.

### 5.3.6.1 Ongoing Monitoring

The Copyright Directive provides for a system to monitor the impact of Article 6. Article 12.1 requires the Commission every three years to submit to the European Parliament, the Council, and the Economic and Social Committee a report on the application of the Directive. The first report had to be submitted by 22 December 2004. In particular, this report must examine whether article 6 ‘confers a sufficient level of protection and whether acts which are permitted by law are being adversely affected by the use of effective technological measures’. The Commission should report not only on article 6 but also on articles 5 and 8 ‘in the light of the development of the digital market’.

Article 12.1 also states that the Commission, where necessary and in particular to ensure the functioning of the internal market, must submit proposals for amendments of the Directive. Article 12.1 further provides for the establishment of a ‘contact committee’, which has the specific task to ‘act as a forum for the assessment of the digital market in works and other items, including private copying and the use of technological measures’. This monitoring process is analogous to the rule-making procedure under the DMCA.<sup>152</sup>

Section 12.1 is similar to section 1201(a)(1)(C) of the United States Copyright Act, which provides that during the first two years, and during each succeeding three-year period, the Librarian of Congress should determine in a rule-making proceeding of whether users are likely to be adversely affected in their ability to make non-infringing use through the prohibition of circumventing access measures.

Van Coppenhagen<sup>153</sup> believes that the need for such a monitoring process could have been obviated by prohibiting acts of circumvention that have an infringing purpose.

### 5.3.6.2 The Savings Clause

Article 12.2 of the Copyright Directive states that the ‘[p]rotection of rights related to

---

<sup>152</sup> Van Coppenhagen op cit note 127 at 445.

<sup>153</sup> Ibid.

copyright under this Directive shall leave intact and shall in no way affect the protection of copyright’.

As the protection of rights under the Directive does not affect copyright protection, it seems to follow that the defences and exceptions available under traditional copyright law should also be available against an action based on the violation of article 6. But this is not the case. Article 6 imposes liability for violations over and above liability for copyright infringement. Also, in article 8, the Directive makes available sanctions and remedies in additions to the sanctions and remedies for copyright infringement.

Article 12.2 accordingly does not allow a person who violates article 6 to raise the same defences available under copyright law. Remember that a violation of article 6 is unlawful regardless of whether it results in copyright infringement.

These provisions correspond to section 1201(c)(1) and (2) of the United States Copyright Act.

### **5.3.6.3 Exceptions to Legitimize Circumvention**

Most European systems of copyright exceptions provide for a list of instances where the author is not allowed to enforce her rights. These are closed lists of exceptions, bordered by narrowly defined and exhaustive cases. However, although the Continental systems look alike in the way in which they compile these closed lists of exceptions, the content of these lists is quite different. In Europe, then, exceptions to copyright are diverse and not harmonized.<sup>154</sup>

Initially, in the Proposal and Amended Proposal, the term ‘authority’ in clause 6.1 referred not only to acts authorized by authors but also to acts authorized by law. The latter reference is, of course, to copyright exceptions. The final text of article 6.1 of the Copyright Directive eliminates the words ‘without authority’. If left like this, article 6.1 would have created a technical monopoly over all uses of copyright works, lawful and unlawful. However, the

---

<sup>154</sup> Séverine Dusollier ‘Exceptions and Technological Measures in the European Copyright Directive of 2001 – An Empty Promise’ (2003) 34 *ICC* 62 at 64-65.

phrase ‘without authority’ appears in article 6.4.<sup>155</sup> Unlike the ‘without authority’ language of the earlier texts, article 6.4 does not refer to general copyright exceptions. So one cannot assume that a copyright exception would necessarily also be an exception to the circumvention prohibition. By incorporating some of the exceptions stated in article 5 of the Directive, article 6.4 now contains specific exceptions to the circumvention prohibition. These exceptions are not as detailed as those created by the DMCA, but they approach the latter in complexity.

The exceptions in article 6.4(1) and (2) apply only to article 6.1 (the prohibition on the *act* of circumvention). This means that although circumvention for the specified lawfully excepted uses must be protected by Member States, circumventing devices or services are excluded from their scope. However, unlike the system enacted by the DMCA, this does not mean that excepted users are deprived of the means with which to perform their excepted acts of circumvention. As I explained above, only the trafficking in circumvention devices used for commercial purposes are prohibited, not devices manufactured exclusively to perform excepted acts of circumvention.

Article 6.4 incorporates some of the exceptions contained in article 5. The latter contains a series of mostly permissive measures aimed at harmonising the limitations and exceptions to the reproduction right, the right of communication to the public, and the right of making available to the public. The exceptions set out in article 5 are exhaustive. This means that if any Member State exception does not fall within the scope of the list, it must be removed.<sup>156</sup> Only one of the article 5 exceptions is mandatory. This lack of harmonization of the exceptions can hinder harmonizing EC copyright law.<sup>157</sup> Article 6.4 aims at facilitating the exercise of some of the limitations to be found in article 5, while at the same time upholding the integrity of technological protection measures.<sup>158</sup>

So far it seems as if the Directive preserves traditional copyright exceptions (unlike the DMCA). But it may be an empty promise. In the first instance, the Directive does not allow

---

<sup>155</sup> Casellati op cit note 22 at 376.

<sup>156</sup> Hart op cit note 68 at 169.

<sup>157</sup> Ibid.

<sup>158</sup> Waelde op cit note 129 at 9.

for the circumvention of access controls. Secondly, the implementation of these specific exceptions and limitations is not mandatory, and so could leave the legislation of Member States unharmonized.<sup>159</sup> This, in turn, could hinder technology industries in the development of copy protection systems, because the lack of harmonization means that a new technical measure that block uses may be perfectly lawful in some countries but not in others.<sup>160</sup>

### 5.3.6.3.1 Certain Copyright Exceptions

Article 6.4(1) of the Copyright Directive reads as follows:

‘In the absence of voluntary measures taken by [authors], including agreements between [authors] and other parties concerned, Member States shall take appropriate measures to ensure that [authors] make available to the beneficiary of an exception or limitation. . . , the means of benefiting from the 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 or subject-matter concerned.’

Article 6.4(1) clarifies that the preferred solution to protect digital copyright is voluntary measures taken by authors. These voluntary measures should allow for certain specific exceptions or limitations as provided for in national law.<sup>161</sup> The State should intervene only in the absence of such measures.<sup>162</sup> In the absence of these measures within a reasonable period of time,<sup>163</sup> Member States are obliged to take appropriate measures to ensure that authors provide beneficiaries of such exceptions or limitations with appropriate means of benefiting from them, by modifying an implemented technological protection measure or by other means.<sup>164</sup>

The Directive does not define the term ‘voluntary measures’. It merely states that these measures include agreements between authors and other parties concerned. The reference to

---

<sup>159</sup> Hart op cit note 68 at 170; Lipton op cit note 2 at 348.

<sup>160</sup> Hart op cit note 68 at 170.

<sup>161</sup> Specifically, art 5.2(a), (c), (d) and (e), and art 5.3(a), (b) and (e) of the Copyright Directive op cit note 6.

<sup>162</sup> Dusollier op cit note 154 at 63.

<sup>163</sup> Recital 51 of the Copyright Directive op cit note 6.

agreements envisages licensing agreements and special laws to ensure the availability of works for public purposes. It would appear that by ‘voluntary measures’ the drafters envisaged technologies that are sufficiently transparent to permit easy access for lawful purposes.<sup>165</sup>

According to Dussolier,<sup>166</sup> ‘building copyright exceptions by design’ is a key example of such a voluntary measure. Authors could devise technological protection measures to accommodate some exceptions. According to her, this implies that the exceptions are given a positive, and not only a defensive, character. This would be the first time that authors have been asked to facilitate the exercise of exceptions to their rights.

It is also unsure what such ‘appropriate measures’ would be in practice. Would a Member State actually legislate to oblige an author to adapt her technological protection device to permit an exception to be exercised? Would an official simply have a quiet word with the relevant author? If so, would it have any effect? If a Member State did nothing, can its government be sued by consumer groups for non-compliance with the mandatory obligation of article 6.1?<sup>167</sup>

Article 6.4(1) uses the peremptory verb ‘shall’ – if the conditions identified in this paragraph are present, Member States are obliged to take the measures indicated. This paragraph expressly states that these exceptions and limitations will be made available only ‘where that beneficiary has legal access to the protected work or subject-matter concerned’. It provides, therefore, that the general anti-circumvention rule of article 6.1 does not apply when legal access has been gained, and if the person concerned is a beneficiary of an exception.<sup>168</sup>

The first requirement, then, is that the beneficiary should have ‘legal access to the protected work’. The term ‘legal access’ is not defined in the Directive. So the meaning of this term should be gleaned from the terms and conditions of the agreement between the author and the

---

<sup>164</sup> Hart op cit note 119 at 62.

<sup>165</sup> Van Coppenhagen op cit note 127 at 444.

<sup>166</sup> Dusollier op cit note 154 at 63.

<sup>167</sup> Hart op cit note 119 at 62-63.

<sup>168</sup> Casellati op cit note 22 at 377.

user – from the law of contract.<sup>169</sup> Lipton<sup>170</sup> remarks that if the term ‘legal access’ were to refer to a beneficiary with a right to access the work and who has technically managed to access the work despite the technological protection measure, this provision adds little to the position in the United States after the enactment of the DMCA. However, as she correctly remarks, such an interpretation does seem rather nonsensical. Perhaps ‘legal access’ in this context is simply been intended to connote a legal right.<sup>171</sup>

It would accordingly appear as if the help given in respect of exercising the exception refers to overcoming copy control but not access control.<sup>172</sup> This would imply that although a user may circumvent copy control, this is an empty promise, as she is not entitled to overcome the access control and so gain access to the protected work. The position under the Directive appears to be the same as that under the DMCA in so far as the protection of access control and the prohibition against circumventing such controls is concerned.<sup>173</sup> Since the act of circumvention is forbidden to gain access, a legitimate user may not circumvent an access control in order to exercise an exception.

The second requirement is that the person should be a ‘beneficiary of an exception or limitation provided for in national law in accordance with Article 5(2)(a), (2)(c), (2)(d), (2)(e), (3)(a), (3)(b) or (3)(e). . .’.

The use must also be limited to the achievement of the purpose of the exception.

A Member State must intervene *only* to enforce the following seven exceptions:

*Repography*: In terms of article 5.2(a), Member States may provide for an exception to the reproduction right ‘in respect of reproductions on paper or any similar medium, effected by the use of any kind of photographic technique or by some other process having similar effects, with the exception of sheet music, provided that the [authors] receive fair

---

<sup>169</sup> Ibid.

<sup>170</sup> Lipton op cit note 2 at 360.

<sup>171</sup> Idem at 361.

<sup>172</sup> Waelde op cit note 129 at 9.

<sup>173</sup> Ibid.

compensation’.

*Reproduction made by publicly accessible libraries, educational establishments or museums, or by archives:* In terms of article 5.2(c), Member States may provide for an exception to the reproduction right ‘in respect of specific acts of reproduction made by publicly accessible libraries, educational establishments or museums, or by archives, which are not for direct or indirect economic or commercial advantage’.

Limiting this exception to establishments ‘which are not for direct or indirect economic commercial advantage’ is far too restrictive – the phrase ‘indirect economic commercial advantage’ can cover many things.<sup>174</sup>

*By broadcasting organizations for ephemeral recordings:* Article 5.2(d) allows Member States to provide for an exception to the reproduction right ‘in respect of ephemeral recordings of works made by broadcasting organisations by means of their own facilities and for their own broadcasts; the preservation of these recordings in official archives may, on the grounds of their exceptional documentary character, be permitted’.

*Reproduction of broadcasts by social institutions:* In terms of article 5.2(e), Member States may provide for an exception to the reproduction right in respect of reproductions of broadcasts made by social institutions pursuing non-commercial purposes, such as hospitals or prisons, on condition that the [authors] receive fair compensation.”

*Reproduction or communication to the public for the sole purpose of illustration for teaching or scientific research:* Article 5.3(a) allows Member States to provide for an exception to the reproduction right and the right of communication to the public for ‘use for the sole purpose of illustration for teaching or scientific research, as long as the source, including the author’ name, is indicated, unless this turns out to be impossible and to the extent justified by the non-commercial purpose to be achieved’.

---

<sup>174</sup> Hart op cit note 68 at 170. Although Hart comments on the Proposal, his remarks apply with equal force to the Copyright Directive.

Unlike the exception relating to fair dealing for research or private study in the United Kingdom,<sup>175</sup> the Directive narrows down its exception to ‘the sole purpose of illustration for teaching or scientific research’. From the phrasing of this provision it is unclear whether it covers scientific research, generally, or only illustration for scientific research.<sup>176</sup> It is also unclear who is entitled to this exception – a single user, or her employer?<sup>177</sup>

Whereas article 5.2(c) expressly limits its beneficiaries to educational institutions, article 5.3(a) goes wider and applies to any non-commercial teaching and research. Also, the former provision is an exception to the reproduction right only, whereas the latter applies in respect of both reproduction right and the right of communication to the public.<sup>178</sup>

*Reproduction or communication to the public for people with disabilities:* In terms of article 5.3(b), Member States may limit the reproduction right and the right of communication to the public in respect of ‘uses, for the benefit of people with a disability, which are directly related to the disability and of a non-commercial nature, to the extent required by the specific disability’.

The Proposal sought to restrict this exception to visual or hearing disability.

Two requirements fence in this exception: the excepted use should be non-commercial, and only to the extent required by the disability in question.<sup>179</sup>

*Reproduction or communication to the public for public security or official uses:* Article 5.3(e) provides that Member States may limit the reproduction right and the right of communication to the public in respect of ‘use for the purposes of public security or to ensure the proper performance or reporting of administrative, parliamentary or judicial proceedings’.

---

<sup>175</sup> Section 29 of the Copyright, Designs and Patents Act 1988.

<sup>176</sup> Hart op cit note 68 at 170. Although Hart comments on the Proposal, his remarks apply with equal force to the Copyright Directive.

<sup>177</sup> Casellati op cit note 22 at 397.

<sup>178</sup> Ibid.

<sup>179</sup> Hart op cit note 68 at 170. Although Hart comments on the Proposal, his remarks apply with equal force to the Copyright Directive.

Hugenholtz<sup>180</sup> criticizes these exceptions, with reason, on the basis that all the exceptions allowed under article 5 are optional, not mandatory (apart from those under article 5.1). (This exception does not apply to the circumvention of technological protection measures.) Also, Member States are not obliged to enact the full list of exceptions. This defeats the purpose of harmonizing European law,<sup>181</sup> which lack of harmonization exacerbates legal uncertainty.<sup>182</sup>

Hugenholtz<sup>183</sup> also objects to the notion of a closed list of limitations. He says that the Internet produces new business models and new uses almost every day. Many of these exceptions are drafted in inflexible technology specific language. If some unforeseen use that everyone agree should be exempted should emerge, it will take at least three years for the Directive to be amended.

Recital 51 tries to shed some light on article 6.4(1):

‘The legal protection of technological protection measures applies without prejudice to public policy, as reflected in Article 5, or public security. Member States should promote voluntary measures taken by [authors], including the conclusion and implementation of agreements between [authors] and other parties concerned, 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 to ensure that [authors] provide beneficiaries of such exceptions or limitations with appropriate means of benefitting from them, by modifying an implemented technological measure or by other means. However, in order to prevent abuse of such measures taken by [authors], including within the framework of agreements, or taken by a Member State, any technological measures applied in the implementation of such measures should enjoy legal protection.’

---

<sup>180</sup> Hugenholtz op cit note 5 at 501.

<sup>181</sup> Coen van Laer ‘Open Forum: The New European Copyright Directive’ (2001) 29 *International Journal of Legal Information* xlvii- xlix at xlix agrees with Hugenholtz: ‘The harmonization of copyright law will not be achieved because of the twenty optional exceptions.’

<sup>182</sup> Idem at xlix.

Unfortunately, this recital does not address the questions raised above. It also does not answer three interdependent questions. In the first instance, for what specific reasons have the exceptions and limitations in article 6.4(1) been found to be matters of public policy? Secondly, why are Member States obliged to ensure the applicability of those exceptions and limitations through ‘appropriate measures’ when, under article 6.4(2), those exceptions and limitations are optional? Thirdly, if it was found that those exceptions and limitations, because of the considerations of public policy stated in recital 51, should always prevail, if necessary also by removing the possible ‘obstacles’ created by technological measures, why has the Directive not made their application obligatory (subject, of course, to the ‘three-step test’ in article 6.4(5)? However, seeking answers to these questions may be purely an intellectual exercise – in practice, Member States do provide in their national laws for these exceptions and limitations.<sup>184</sup>

Article 6.4(1) can be given its full meaning only if it is read together with article 6.4(4): the obligation to make a work available to lawful users may not be imposed on an author where the work in question is distributed on demand online, and there is a contract prohibiting the act. So if it is feasible to regulate the use of a work contractually and to block its use technologically, then market forces prevail. It seems, then, as if the Directive implies that the copyright exceptions are of no importance when the excepted use is technologically controlled and the user agrees contractually not to perform the excepted act (put differently, when the transaction cost does not prevent entering into a contract).<sup>185</sup>

However, these provisions need further clarification. What happens if users do not accept the contractual terms? May the works still be regarded as having been offered on contractual terms? Ficsor<sup>186</sup> believes that it would not be appropriate to answer the latter question in the negative if the terms offered are sufficiently reasonable. So it would certainly not be enough for the Member States merely to observe the absence of ‘voluntary measures’ and then to conclude without further ado that they have to intervene as article 6.4(1) ‘obliges’ them to

---

<sup>183</sup> Hugenholtz op cit note 5 at 501.

<sup>184</sup> Ficsor op cit note 34 para 11.29 at 560-561.

<sup>185</sup> Kamiel J Koelman ‘The protection of technological measures vs. the copyright limitations’ paper presented at the ALAI Congress Adjuncts and Alternatives for Copyright, New York, 15 June 2001 available at <<http://www.ivir.nl/publications/koelman/alaiNY.html>>. See specifically note 11.

dol. The purpose of this complex regulation is clearly to give priority to contractual arrangements, and this policy seems to be correct. If the parties are left to themselves for a while, they will certainly be able to work out appropriate arrangements with due attention to the specific features of the acts covered by the exceptions and limitations listed in article 6.4(1). Perhaps the spectre of the application of the measures mentioned this provision will act as a useful catalyst to promote agreement.<sup>187</sup>

To summarize: Hugenholtz<sup>188</sup> says the following about the implementation of article 6.4(1) in practice:

‘I have read and reread this text several times, but most of it still eludes me. What “voluntary measures” does the Directive envisage: technical protection measures that automatically respond to eligible users? And what kind of “agreements between rightholders and other parties” do the framers of the Directive have in mind? Collective understandings between rightholders and users? And, if such measures and agreements are not in place (within what timeframe?), which kind of “appropriate measures” are the Member States expected to take? Does the Directive call for voluntary deposit of analogue copies, available for public inspection and reproduction in national libraries? Or, are Member States obliged to effectively prohibit the use of technological protection schemes if public access to work is impaired on a serious scale?’

According to Casellati,<sup>189</sup> a possible solution to the problem of vagueness encountered in these exceptions is for Member States to identify bodies or institutions that are entitled to request such circumvention tools. To make mandatory exceptions work, the determination should be as specific and as narrow as possible.

Caselatti<sup>190</sup> refers to two possible solutions offered in the United States to ensure fair use –

---

<sup>186</sup> Ficsor op cit note 34 para 11.29 at 561.

<sup>187</sup> Ibid.

<sup>188</sup> Hugenholtz op cit note 5 at 501.

<sup>189</sup> Casellati op cit note 22 at 398.

<sup>190</sup> Ibid.

(a) trying to ‘code fair use’, and (b) providing for a ‘key escrow’ to be administered by a trusted third party that would release keys to applicants. Application for keys to circumvent technological protection measures for purposes of fair use would be made to the third party, rather than directly to an individual author. Caselatti believes that structure might also be imposed in the EC. The safe harbour provisions would be represented by private agreements between authors and third parties, whereas the role of the Library of Congress could be played by the Contact Committee created under article 12 of the Copyright Directive, the Electronic Copyright Management System, or authors’ collecting societies at the national level.<sup>191</sup>

### **5.3.6.3.2 Private Copying**

Article 6.4(2) of the Copyright Directive deals with private copying. The reason for treating private copying separately is the controversy among the Member States as to the proper treatment of the relationship between technological protection measures and private digital copying.<sup>192</sup>

The issue was whether digital private copying should be treated differently from analogue private copying. Some Member States believed that digital private copying should indeed be treated differently from analogue private copying, and that an exception to allow digital private copying should be eliminated as soon as effective technological protection measures were established. Others wanted to allow for some degree of digital copying combined with remuneration schemes in view of the possibility of limiting the number of copies through technological protection measures.<sup>193</sup>

Apparently there was no consensus. Article 6.4(2) reads as follows:

‘A Member state may also take such measures in respect of a beneficiary of an exception or limitation provided for in accordance with Article 5(2)(b), unless

---

<sup>191</sup> Ibid.

<sup>192</sup> Idem at 379.

<sup>193</sup> Idem at 379.

reproduction for private use has already been made possible by [authors] to the extent necessary to benefit from the exception or limitation concerned and in accordance with the provisions of Article 5(2)(b) and (5), without preventing [authors] from adopting adequate measures regarding the number of reproductions in accordance with these provisions.’

With regards to digital private copying, the phrase ‘without preventing [authors] from adopting adequate measures regarding the number of reproductions in accordance with these provisions’ makes it clear that digital private copying is not prohibited, and rejects the coexistence of digital private copying and technological protection measures.<sup>194</sup>

The use of the permissive ‘may’ in article 6.4(2) indicates a different thinking from that in article 6.4(1) where the peremptory ‘shall’ is used. ‘May’ suggests that each Member State has the discretion to decide whether or not to implement the private copying exception in national law.<sup>195</sup> Accordingly, if a technological protection measure were to be introduced to prevent television viewers from recording a programme for purposes of time shifting, a Member State would not be obliged to do anything about it.<sup>196</sup>

Recital 38 confirms that Member States are free to choose whichever approach they prefer:

‘Digital private copying is likely to be more widespread and have a greater economic impact. Due account should therefore be taken of the differences between digital and analogue private copying and a distinction should be made in certain respects between them.’

The burden on a Member State to intervene under article 6.4(2) is less onerous than under article 6.4(1).

In the first instance, as I have just indicated, the use of the word ‘may’ in the former confers a

---

<sup>194</sup> *Idem* at 382.

<sup>195</sup> *Ibid*; Hart op cit note 119 at 63.

<sup>196</sup> Hart op cit note 119 at 63.

discretion, as opposed to the obligation imposed by ‘shall’ in the latter. As a whole, article 6.4(2) can be read as preferring private ordering (contract).<sup>197</sup>

Secondly, a Member State may intervene only to the extent necessary to achieve the purpose of an exception.<sup>198</sup>

Thirdly, a further limitation on state intervention concerns the impossibility of prohibiting authors from adopting ‘appropriate measures regarding the number of reproductions’. This limitation refers to technological measures that limit or control the number of reproductions (such as the Serial Copy Management System (SCMS), which allows copies to be made from the original but not from another copy).<sup>199</sup>

Fourthly, article 6.4(2) requires compliance with articles 5.2(*b*) and 5.5, which further limits state intervention. Although every exception in article 5 has to comply with the three-step test in article 5.5, article 6.4(2) expressly contains an additional reference to article 5.5 in order to strengthen the import of this test.<sup>200</sup>

Article 5.2(*b*) allows Member States to limit the reproduction right ‘in respect of reproductions on any medium made by a natural person for private use and for ends that are neither directly nor indirectly commercial, on condition that the [authors] receive fair compensation which takes account of the application or non-application of technological measures referred to in Article 6 to the work or subject-matter concerned’.

Recital 52 reads as follows:

‘When implementing an exception or limitation for private copying in accordance with Article 5(2)(*b*), Member States should likewise promote the use of voluntary measures to accommodate achieving objectives of such exception or limitation. If, within a reasonable period of time, no such voluntary measures to make reproduction

---

<sup>197</sup> Ficsor op cit note 34 para 11.29 at 560-561.

<sup>198</sup> Casellati op cit note 22 at 382.

<sup>199</sup> Idem at 382-383.

<sup>200</sup> Idem at 383.

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. Voluntary measures taken by [authors], including agreements between [authors] and other parties concerned, as well as measures taken by Member States, do not prevent [authors] from using technological measures which are consistent with the exceptions or limitations on private copying in national law in accordance with Article 5(2)(b), taking account of the condition of fair compensation under that provision and the possible differentiation between various conditions of use in accordance with Article 5(5), such as controlling the number of reproductions. In order to prevent abuse of such measures, any technological measures applied in their implementation should enjoy legal protection.’

The wording of article 5.5<sup>201</sup> is almost identical to that of article 9.2 of the Berne Convention. The criteria of this three-step test are: (a) the exception must relate to ‘certain special cases’; (b) the excepted use cannot conflict with a normal exploitation of the work in question; and (c) there must not be unreasonable prejudice to the author’s legitimate interests.

According to Caselatti,<sup>202</sup> an exception for digital private copying can be challenged on the ground that it is not a ‘special case’ – it is not justified by public policy or other exceptional circumstances. Regarding the second and third steps of the test, the more digital private copying is limited by technology and the higher the compensation payable, the greater the possibility that this exception will pass muster.

If it were to be found that a Member State’s exception in relation to digital private copying does not pass the three-step test, such exception would be null and void. And, if Casellati’s<sup>203</sup> interpretation of the decision of the WTO dispute resolution panel<sup>204</sup> regarding the three-step

---

<sup>201</sup> Article 5.5 provides: ‘The exceptions and limitations provided for in paragraphs 1, 2, 3 and 4 shall only be applied in certain special cases which do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the [author].’

<sup>202</sup> Casellati op cit note 22 at 386. On pages 383-385 she discusses the interpretations of the WTO dispute resolution panel before reaching this conclusion.

<sup>203</sup> Idem at 383-385.

<sup>204</sup> In a dispute between the European Union and the United States of America over an exception to the right-holders’ copyright in US copyright law (WT/DS160/R of 15 June 2000) accessible at <[http://wto.org/english/tratop\\_e/dispu\\_e/1234da.pdf](http://wto.org/english/tratop_e/dispu_e/1234da.pdf)> (last visited on 28 March 2007).

test is correct, it seems as if the room for Member States' to allow for digital private copying exceptions is very limited indeed.

### 5.3.6.3.3 Circumvention Devices Made Available by Authors

Article 6.4(3) was introduced in May 2000.<sup>205</sup> It reads as follows:

‘The technological measures applied voluntarily by [authors], including those applied in implementation of voluntary agreements, and technological measures applied in implementation of the measures taken by Member States, shall enjoy the legal protection provided for in paragraph 1.’

This paragraph extends the legal protection article 6.1 to those measures applied under article 6.4(1) and (2). These paragraphs create exceptions to the circumvention prohibition and provide for circumvention tools. Article 6.4(3) accordingly extends protection to circumvention tools similar to that in article 6.1 for technological protection measures. Two types of circumvention tools are protected – those provided by authors of their own accord or in performance of voluntary agreements, and those provided by Member States in the absence of such agreements.

Recital 51 explains that ‘in order to prevent abuse of such measures . . . any technological measures applied in implementation of such measures should enjoy legal protection’.

According to Casellati,<sup>206</sup> the protection provided for in article 6.1 would be frustrated without article 6.4(3).

She<sup>207</sup> also refers to article 6.2(a) and (b) of the Computer Programs Directive:<sup>208</sup> in order to achieve the interoperability of a computer program with other programs it is stated that information obtained for this purpose should not be used for other goals, nor given to others.

---

<sup>205</sup> Casellati op cit note 22 at 386n46.

<sup>206</sup> Idem at 386.

<sup>207</sup> Ibid.

<sup>208</sup> The Computer Programs Directive op cit note 35.

So this Directive allows circumvention to obtain certain knowledge but prohibits the distribution of the information. By prohibiting such distribution, it protects the information. The protection of the circumvention tools under article 6.4(3) of the Copyright Directive accordingly not foreign to EC law. The difference between these Directives is that in the Computer Programs Directive the end user is allowed directly to circumvent, whereas in the Copyright Directive the circumvention tools are provided by the author or Member State.<sup>209</sup>

#### **5.3.6.3.4 The Interface of Copyright Law and the Law of Contract**

Article 6.4(4) of the Copyright Directive was proposed at the end of May 2000, just two weeks before the Political Agreement of the European Council on the Directive.<sup>210</sup> It states that '[t]he provisions of the first and second subparagraphs shall not apply to works or other subject-matter made available to the public on agreed contractual terms in such a way that members of the public may access them from a time and place and at a time individually chosen by them'.

This paragraph significantly restricts the scope of article 6.4(1) (2).

The exclusive right to make works 'available to the public . . . in such a way that members of the public may access them from a place and at a time individually chosen by them' is a new right created by article 3.2. In terms of the Explanatory Memorandum,<sup>211</sup> this right addresses the interactive on-demand acts of transmission. It excludes every type of broadcast for which the pre-defined programs do not meet the 'individual choice' requirement (such as 'pay TV' or 'pay per view'), and also the 'near video on demand' services, where a program is broadcast several times at short intervals.<sup>212</sup>

Article 6.4(4) specifies that, in the case of on-demand services, freedom of contract prevails over the copyright exceptions. The literal meaning of this provision clearly excludes the exceptions set out in article 6.4(1) and (2).

---

<sup>209</sup> Casellati op cit note 22 at 386n47.

<sup>210</sup> Idem at 386.

<sup>211</sup> Explanatory Memorandum, Copyright Directive op cit note 6.

<sup>212</sup> Casellati op cit note 22 at 387.

In the past it was unclear whether the law of contract could inhibit the availability of copyright exceptions. These doubts have now been cast aside by the Copyright Directive: it states that paragraphs (1) and (2) of article 6.4 'shall not apply' to works made available 'agreed contractual terms' by way of interactive on-demand services. From this follows that the law of contract prevails.

Recital 53 states that

'[t]he protection of technological measures should ensure a secure environment for the provision of interactive on-demand services, in such a way that members of the public may access works or other subject-matter from a place and at a time individually chosen by them. Where such services are governed by contractual arrangements, the first and second subparagraphs of Article 6.4 do not apply. Other forms of non-interactive online use remain subject to those provisions.'

Recital 53 does not give much guidance to the interpretation of article 6.4(4). Rather, the phrase '[w]here such services are governed by contractual arrangements' suggests that there are certain on-demand services that are not governed by contractual arrangements. If this is so, it would mean that two different legal regimes would apply to on-demand services, depending on whether such services are governed by contractual arrangements. On-demand services are usually governed by some sort of 'click on' licence. It is difficult to imagine that such a licence would not be considered to be a contractual arrangement. So it seems as if every on-demand service would be regulated by the law of contract.<sup>213</sup> Some authors<sup>214</sup> accordingly regard the protection of technological measures as an over protection of authors to the detriment of users – authors benefit not only from technological protection measures and their legal protection but also from the law of contract.

Online contracts are usually presented as contracts of adhesion, on a 'take it or leave it' basis.

---

<sup>213</sup> *Idem* at 388-389; Hart *op cit* note 119 at 63.

<sup>214</sup> Kamiel Koelman & Natali Helberger 'Protection of Technological Measures' *IMPRIMATUR* (Nov 1998) at 25 available at <<http://imprimatur.net/download.htm>>, cited by Casellati *op cit* note 22 at 389.

This raises concerns for users who would not be able to negotiate, or who could be uninformed about the content of the agreement.<sup>215</sup> Casellati<sup>216</sup> does not think that this is crucial – if the user decides to pay for a service, she must have concluded that it would be beneficial to her. Also, the wording of paragraph (4) refers expressly to ‘agreed’ contractual terms. A narrow reading of this provision may protect consumers against unfair contracts of adhesion.

Furthermore, Casellati<sup>217</sup> points out that the EC already has mechanisms to deal with abusive consumer contracts. She refers to article 3.1 of the Directive on Unfair Terms in Consumer Contracts,<sup>218</sup> which provides that ‘a contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties’ rights and obligations arising under the contract, to the detriment of the consumer’. Also, article 6 of the Directive on the Protection of Consumers in Respect of Distance Contracts<sup>219</sup> requires a seven-day cooling-off period, which allows a consumer to terminate the agreement without giving reasons. And it provides, in article 12.2, that ‘Member States shall take the measures needed to ensure that the consumer does not lose the protection granted by this Directive by virtue of the choice of law of a non-member country as the law applicable to the contract if the latter has close connections with the territory of one or more Member States’.

In a nutshell, then, article 6.4(4) establishes that, in relation to on-demand services, the copyright exceptions do not apply and the law of contract prevails.

Interactive on-demand use is presently the most important use of works protected by copyright in an online environment. It seems as if article 6.4(4) severely compromises the attempt by the drafters of the Directive to deal with the exceptions to copyright.

---

<sup>215</sup> Institute for Information Law ‘Contracts and Copyright Exemptions’ IMPRIMATUR (December 1997) available at <<http://www.imprimatur.net/download.htm>> cited by Casellati op cit note 22 at 389.

<sup>216</sup> Casellati op cit note 22 at 389.

<sup>217</sup> Ibid.

<sup>218</sup> Council Directive 93/13/1993 OJ (L 95) 29 (5 April 1993) on Unfair Terms in Consumer Contracts, cited by Casellati op cit note 22 at 389.

<sup>219</sup> Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the Protection of

The provision also raises the issue of the enforceability of electronic contracts that override copyright exceptions, as it allows an author effectively to impose her own conditions on each end user without considering the copyright balance.<sup>220</sup> The main problem with article 6.4(4) is that it allows the parties to contract out of the benefit conferred by copyright law in the form of an exception.

### **5.3.6.3.5 The Relationship Between Article 6.4 and Other Directives**

Article 6.4(5) of the Copyright Directive states that ‘[w]hen this Article is applied in the context of Directives 92/100/EC and 96/9/EC this paragraph shall apply *mutatis mutandis*’.

This paragraph refers expressly to the Rental/Loan<sup>221</sup> and the Database<sup>222</sup> Directives, and clarifies that the Copyright Directive prevails over these other Directives. But it does not specify the relationship between the protection of technological protection measures and the Computer Programs Directive.<sup>223</sup>

Recital 50 provides:

‘Such an harmonized legal protection does not affect the specific provisions on protection provided for by Directive 91/250/EEC. In particular, it should not apply to the protection of technological measures used in connection with computer programs, which is exclusively addressed in that Directive. It should neither inhibit nor prevent the development or use of any means of circumventing a technological measure that is necessary to enable acts to be undertaken in accordance with the terms of Article 5(3) or Article 6 of Directive 91/250/EEC. Articles 5 and 6 of that Directive exclusively determine exceptions to the exclusive rights applicable to computer programs.’

In terms of this recital, then, the Computer Programs Directive continues to be applied. The

---

Consumers in Respect of Distance Contracts. Casellati op cit note 22 at 389.

<sup>220</sup> Van Copenhagen op cit note 127 at 444-445.

<sup>221</sup> The Rental Right Directive op cit note 57.

<sup>222</sup> The Database Directive op cit note 57.

<sup>223</sup> The Computer Programs Directive op cit note 35.

recital also specifies the consequences of this application in the digital environment: Member States can neither ‘inhibit nor prevent the development or use of any means of circumventing a technological measure that is necessary to enable acts to be undertaken’ in reference to article 5.3 (reverse engineering) and article 6 (decompilation).

Article 5 of the Computer Programs Directive provides for ‘[e]xceptions to the restricted acts’. Article 5.3 reads as follows:

‘The person having a right to use a copy of a computer program shall be entitled, without the authorization of the [author], to observe, study or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program if he does so while performing any of the acts of loading, displaying, running, transmitting or storing the program which he is entitled to do.’

Article 6 of the Computer Programs Directive allows for decompilation to achieve interoperability:

‘1. The authorization of the rightholder shall not be required where reproduction of the code and translation of its form within the meaning of Article 4 (a) and (b) are indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs, provided the following conditions are met:

- (a) these acts are performed by the licensee or by another person having a right to use a copy of a program, or on their behalf by a person authorized to do so;
- (b) the information necessary to achieve interoperability has not previously been readily available to the persons referred to in subparagraph (a); and
- (c) these acts are confined to the parts of the original program which are necessary to achieve interoperability.

‘2. The provisions of paragraph 1 shall not permit the information obtained through its application:

- (a) to be used for goals other than to achieve the interoperability of independently

- created computer programs;
- (b) to be given to others, except when necessary for the interoperability of the independently created computer program; or
  - (c) to be used for the development, production or marketing of a computer program substantially similar in its expression, or for any other act which infringes copyright.

‘3. In accordance with the provisions of the Berne Convention for the protection of Literary and Artistic Works, the provisions of this Article may not be interpreted in such a way as to allow its application to be used in a manner which unreasonably prejudices the rightholder’s legitimate interests or conflicts with a normal exploitation of the computer program.’

The continued application of the Computer Programs Directive has the result that article 6.4 of the Copyright Directive (which allows contractual agreements to override copyright exceptions) would not apply to computer software. So it would not be possible to contract out of the reverse engineering and decompilation exceptions. It seems, then, as if the reverse engineering and decompilation of computer programs are effectively two further exceptions to article 6.1 of the Copyright Directive.<sup>224</sup>

Would making back-up copies also be an exception to the circumvention prohibition? Recital 50 refers only to articles 5.3 and 6 of the Computer Programs Directive; it does refer to article 5.2m which deals with making back-up copies. Does this evince an intention to exclude article 5.2? It does, if one applies the *inclusio unius exclusio alterius maxim*. If so, it means that a user entitled to avail herself of the back-up copy exception cannot circumvent a technological protection measure in order to exercise the exception.

According to Casellati,<sup>225</sup> it rather seems that the Copyright Directive states a general principle and clarifies the most pressing issues, in the process stressing the importance of certain exceptions during implementation by Member States. A good reason to her for the

---

<sup>224</sup> Casellati op cit note 22 at 391.

<sup>225</sup> Ibid.

Copyright Directive not expressly mentioning article 5.2 of the Computer Programs Directive is that the back-up copy exception has successfully been implemented in all Member States.

### **5.3.7 Remedies**

Respectful of the division of responsibility between the European Community (First Pillar) and the field of justice and home affairs (Third Pillar) resulting from the Treaty on the European Union, the Copyright Directive does not contain criminal sanctions and procedures, even though the Directive may require that certain infringements of intellectual property be met at the national level by criminal sanctions.<sup>226</sup>

The Directive includes only general, framework-type provisions, as the way in which such remedies may be provided depends largely on the civil or criminal legislation of Member States.

Article 8 of the Directive reads as follows:

‘1. Member States shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in this Directive and shall take all the measures necessary to ensure that those sanctions and remedies are applied. The sanctions thus provided for shall be effective, proportionate and dissuasive.

‘2. Each Member State shall take the measures necessary to ensure that [authors] whose interests are affected by an infringing activity carried out on its territory can bring an action for damages and/or apply for an injunction and, where appropriate, for the seizure of infringing material as well as of devices, products or components referred to in Article 6(2).

‘3. Member States shall ensure that [authors] are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.’

Note that article 8 extends not only to violations of the provisions relating to technological protection measures, but, generally, to any ‘infringements of the rights and obligations set out in this Directive’. Also, in article 8.2 there is a specific obligation to provide for measures necessary, ‘where appropriate’, ‘for the seizure of infringing material as well as of devices, products or components...’.<sup>227</sup>

### **5.3.8 A Summary of the Objections Against Article 6**

I have addressed most of the objections against article 6 in my discussion of the component parts of this article. But for the sake of convenience, I shall summarize below the main objections.

#### **5.3.4.1 The Directive Does Little to Harmonize European Copyright Law**

This assertion is based on several facts, especially that the implementation of exceptions and limitations are not mandatory, the emphasis on parties’ voluntary agreements and freedom of contract, and that computer software as copyright works is subject to a special protection regime under the Computer Programs Directive. Whereas the Copyright Directive prohibits both the act of circumvention and trafficking in circumvention devices, the Computer Programs Directive prohibits only circumvention devices. And the tests for the prohibited devices differ in the two Directives.

However, a positive consequence of computer software not being subject to the Copyright Directive and thus the provisions of article 6.4 is that it would not be possible to contract out of the reverse engineering and decompilation exceptions in the Computer Programs Directive. This will probably prevent in Europe the debate that has occurred in the United States over the enforcement of shrink-wrap or ‘click wrap’ licences that prevent users from enjoying the reverse engineering exception.<sup>228</sup>

---

<sup>226</sup> Ravillard op cit note 4 at 42.

<sup>227</sup> Ficsor op cit note 34 para 11.21 at 554-555.

<sup>228</sup> Casellati op cit note 22 at 400.

### **5.3.4.2 The Directive Does not Preserve Traditional Copyright Exceptions**

The Directive does not allow for the circumvention of access controls, and does not make the implementation of the exceptions mandatory.

### **5.3.4.3 The Negative Implications of the Article 6.4 Contract Regime**

The emphasis on parties' voluntary agreements in article 6.4 could lead to a lack of harmonization. As the law of contract, generally, overrides copyright exceptions in the case of on-demand services, authors who make their works available through on-demand services can contract out of all copyright exceptions and so upset the copyright balance. This could also be detrimental to the free flow of information. If it were possible for the user to access that work off-line, the free flow of information would be guaranteed by access to the hard copies.<sup>229</sup> By contrast, if an author makes a work only available online and contracts out of important public interest exceptions, the user has to resort to litigation in order to enjoy these exceptions. This need to litigate will have a chilling effect on spontaneous uses, and litigation will certainly be costly and lengthy.<sup>230</sup> The general principle emanating from article 6.4 is that freedom of contract prevails over copyright law in the digital environment.<sup>231</sup>

### **5.3.4.4 The Replacement of Copyright Law by Technological Monopolies and Electronic Contracts**

Article 6 could well replace copyright law with technological protection measures or electronic contracts. This, in turn, may lead to market distortions and undermine consumer confidence.<sup>232</sup>

## **5.4 Conclusion**

---

<sup>229</sup> *Idem* at 401.

<sup>230</sup> *Ibid.*

<sup>231</sup> This is consistent with article 9 of the Copyright Directive, which states that '[t]his Directive shall be without prejudice to provisions concerning in particular . . . the law of contract'.

<sup>232</sup> Alex Morrison & Lorna E. Gillies 'Securing Webcast Content in the European Union: Copyright, Technical

Like its United States counterpart, article 6 of the Copyright Directive goes well beyond the obligation created by article 11 of the WCT and prohibits the act of circumvention as well as trafficking in circumvention devices.

At first blush, it seems that article 6 of the Directive, unlike section 1201 of the United States Copyright Act, preserves traditional copyright exceptions because of the long list of stated exceptions. But this is a mirage. In the first instance, the Directive does not allow for the circumvention of access controls, and without access, subsequent use is impossible. Secondly, the implementation of the specific exceptions is not mandatory in Member States.

The main distinction between the Directive and the United States Copyright Act lies in the way in which the Directive provides for electronic contracts. In the Directive, freedom and the sanctity of contract prevail over copyright law in the digital environment. It raises the question, though, as to whether the law of contract can override copyright exceptions established on the basis of public policy.

Hugenholtz<sup>233</sup> argues that the Directive is ‘a badly drafted, compromise-ridden, ambiguous piece of legislation’ that does not create legal certainty, despite this being one of the goals stated in the recitals of the Directive.<sup>234</sup> The Directive certainly does not create legal certainty, nor does it harmonize copyright law in Europe.

The Directive has been implemented widely by the Member States. It is unfortunately too early for any case law on the circumvention prohibition to emerge, in order to see how national courts deal with the circumvention provisions.

---

Protection and Problems of Jurisdiction on the Internet’ [2000] *European Intellectual Property Review* 74 at 79.

<sup>233</sup> Hugenholtz op cit note 5 at 500.

<sup>234</sup> Recitals 4, 6, 7 and 21 of the Copyright Directive.

## CHAPTER 6: SOUTH AFRICA

“That’s the reason they’re called lessons”, the Gryphon remarked: “because they lessen from day to day.””

LEWIS CARROL

*Alice’s Adventures in Wonderland*

### 6.1 Introduction

Although South Africa is a signatory to the WIPO Copyright Treaty (WCT),<sup>1</sup> it has not yet implemented the treaty provisions in national copyright legislation. As I shall show below, however, by a strange quirk South Africa has effectively implemented article 11 of the WCT, albeit not in copyright legislation.

In this chapter I shall consider whether existing South African legislation sufficiently provide for the protection against the circumvention of technological protection measures. As my analysis in previous chapters has shown, it is clear that the implementation of article 11 in the United States and the European Union led to enhance the protection of authors, diminish the opportunity of users to use copyright works, and so, generally, upset the fine copyright balance.

When one has to decide whether South Africa needs legislation to implement the WCT, two questions arise for consideration. In the first instance, does existing legislation discharge our obligations under the WCT? If it does, of course, further implementation legislation would be unnecessary. Secondly, should South Africa decide to amend its current legislation, would it benefit economically and socially from the stronger protection extended to authors?

### 6.2 Digitization and Developing Countries

---

<sup>1</sup> South Africa signed the WCT on 12 December 1997: see [http://www.wipo.int/treaties/en/Remarks.jsp?cnty\\_id=1525C](http://www.wipo.int/treaties/en/Remarks.jsp?cnty_id=1525C) (visited on 27 April 2005).

As I indicated earlier, digitization and information technology made it possible to distribute unlimited quantities of information inexpensively on a world-wide scale. Theoretically, this should benefit developing countries such as South Africa, as it would offer them the opportunity to acquire information and enhance their educational systems at low cost. Unfortunately, though, it seems as if the ‘digital divide’ and the ever-expanding copyright protection legislation make it unlikely that developing countries will benefit from information technology.<sup>2</sup>

What is the ‘digital divide’? The phrase connotes the gap between the information haves (the developed countries) and the information have-nots (the developing and especially the least developed countries). The G8 Digital Opportunity Task Force<sup>3</sup> describes the digital divide as ‘. . . in effect, a reflection of existing broader socio-economic inequalities and can be characterized by insufficient infrastructure, high costs of access, inappropriate or weak policy regimes, inefficiencies in the provision of telecommunication networks and services, lack of locally created content, and uneven ability to derive economic and social benefits from information-intensive activities’. The divide exists because most developing countries cannot build up advanced telecommunications infrastructures and employ well-trained technicians to support the operation of the infrastructures, due to poverty and socio-economic constraints.<sup>4</sup>

Stronger copyright protection, in turn, further restricts developing countries’ access to information. Since these countries are dependant for educational and scientific research purposes upon developed countries’ copyright works, the crushing need of developing countries is wider access to developed countries’ copyright works at the lowest possible cost. The adaptation of traditional copyright principles to meet the demands of the digital environment elevated the level of copyright protection both in developed and developing countries.<sup>5</sup> This stronger copyright protection has been attained, in part, by the legal protection of technological protection measures,

---

<sup>2</sup> Haochen Sun ‘Copyright Law Under Siege: An Inquiry into the Legitimacy of Copyright Protection in the Context of the Global Digital Divide’ (2005) 36 *ICC* 192.

<sup>3</sup> Report of the Digital Opportunity Task Force (DOT Force), ‘Digital Opportunities for All: Meeting the Challenge’ 6 (2001), accessible at <<http://www.g8.utoronto.ca/summit/2001genoa/dotforce1.html>> (last visited on 8 February 2006). See also Sun op cit note 2 at 193 and 193n3.

<sup>4</sup> Sun op cit note 2 at 193.

<sup>5</sup> *Idem* at 195.

the extension of the copyright term in the United States<sup>6</sup> and the European Union,<sup>7</sup> and the legal protection of databases.<sup>8</sup> The elevation of the level of copyright protection will probably widen the digital divide.

The higher level of national copyright protection also attains an international dimension – the United States, especially, uses free trade agreements to raise the level of copyright protection in trading partners beyond that established by the Agreement of Trade-Related Aspects of Intellectual Property Rights (‘the TRIPS Agreement’) and the WCT.<sup>9</sup> Countries with which the United States concludes free trade agreements are required, amongst other things, to adopt United States style protection of technological protection measures.<sup>10</sup>

In this way two of the main copyright exporters – the United States and the European Union – are following an aggressive approach internationally to force trading partners to create in their national copyright legislation protection similar to that obtaining in the United States and Europe.<sup>11</sup> Also, the United States and Europe indulge in forum shifting by moving the negotiating table from transparent multilateral agreements to secret bilateral agreements.<sup>12</sup> In terms of the most-favoured-nation treatment requirement of article 4 of the TRIPS Agreement, members of the World Trade Organization (WTO) are obliged to grant the same level of protection to all other members immediately and unconditionally. So the ‘TRIPS plus’ and

---

<sup>6</sup> The Sonny Bono Copyright Term Extension Act, Pub L No 105-298, 112 Stat 2827 (1998) grants a blanket extension of the copyright term by an additional twenty years.

<sup>7</sup> The Council Directive 93/98/EEC of 29 October 1993 on Harmonizing the Term of Protection of Copyright and Certain related Rights, extends the copyright term applicable in all EU Members States to life of the author plus 70 years after her death.

<sup>8</sup> Article 10.2 of the TRIPS Agreement and article 5 of the WCT require their contracting parties to provide copyright protection of original databases; the European Parliament and Council Directive 96/9/EC of 11 March 1996 on the Legal Protection of Databases, OJ EC L 77 creates a new sui generis right for the creator of a database.

<sup>9</sup> Sun op cit note 2 at 199.

<sup>10</sup> See, for example, the Australia-United States Free Trade Agreement (for the text of the agreement, see <[http://www.ustr.gov/Trade\\_Agreements/Bilateral/Australia\\_FTA/Final\\_Text/Section\\_Index.html](http://www.ustr.gov/Trade_Agreements/Bilateral/Australia_FTA/Final_Text/Section_Index.html)> (visited on 29 January 2007).

<sup>11</sup> For an analysis of the American FTA campaign, see Ralph Fischer ‘The Expansion of Intellectual Property Rights by International Agreement: A Case Study Comparing Chile and Australia’s Bilateral FTA Negotiations With the U.S’ (2006) 28 *Loyola of Los Angeles International and Comparative Law Review* 129; and Christopher Arup ‘The US-Australia FTA: law making on the frontier’ (2004) 29 *Alternative Law Journal* 27.

<sup>12</sup> Sun op cit note 2 at 200-201. For an incisive analysis of forum shifting, see Laurence R Helfer ‘Regime Shifting: The Trips Agreement and New Dynamics of International Intellectual Property Lawmaking’, accessible at <<http://www.law.vanderbilt.edu/faculty/faculty-directory/laurence-r-helfer/download.aspx?id=649>> (visited on 29

‘WCT plus’ standards established in the free trade agreements must also be granted to the nationals of all other WTO member states. The higher standards of protection established in the free trade agreements will thus be awarded to authors from other WTO member states as well. These standards can become the new minima from which a future WTO trade negotiating round will have to proceed.<sup>13</sup> The combination of the most-favoured-nation treatment requirement and bilateral agreements has the effect that the new set of minimum standards of copyright protection spreads faster than would have been the case otherwise.<sup>14</sup>

The maintenance of a global public domain is essential for development in developing countries which are largely dependent upon the free flow of information across national borders for educational and scientific research purposes. Traditionally, in copyright law, the idea/expression dichotomy,<sup>15</sup> the doctrine of exhaustion,<sup>16</sup> and the limited term of protection<sup>17</sup> serve to delineate the private and the public domains, and, in the end, to maintain a healthy public domain.

---

January 2007).

<sup>13</sup> Sun op cit note 2 at 200-201.

<sup>14</sup> Idem at 201.

<sup>15</sup> There is no copyright in ideas (see *Galago Publishers (Pty) Ltd & another v Erasmus* 1989 (1) SA 276 (A) at 293G and 283-284). It is the expression of the idea that is the subject of copyright. The Copyright Act 98 of 1978 (the ‘Copyright Act’). accordingly requires that a work should exist in some or other material form before it qualifies for copyright protection. Section 2(2) states:

‘A work, other than a broadcast or programme-carrying signal, shall not be eligible for copyright unless the work has been written down, recorded, represented in digital data or signals, or otherwise reduced to material form.’

<sup>16</sup> Exhaustion of rights means that the owner of a copy of a copyright work may resell the work if it was legitimately obtained, provided that this copy was originally produced by or with the permission of the author. However, in terms of section 23(2) of the Copyright Act, the author may control the aftermarket in instances of parallel importation:

‘Without derogating from the generality of subsection (1), copyright shall be infringed by any person who, without the license of the owner of the copyright and at a time when copyright subsists in a work –

- (a) imports an article into the Republic for a purpose other than for his private and domestic use;
- (b) sells, lets, or by way of trade offers or exposes for sale or hire in the Republic any article;
- (c) distributes in the Republic any article for the purposes of trade, or for any other purpose, to such an extent that the owner of the copyright in question is prejudicially affected; or
- (d) acquires an article relating to a computer program in the Republic;

if to his knowledge the making of that article constituted an infringement of that copyright or would have constituted such an infringement if the article had been made in the Republic.’

<sup>17</sup> Section 3(2)(a) of the Copyright Act limits the term of protection of literary, musical and artistic works to 50 years after the death of the author. In the case of cinematograph films, photographs, and computer programs the copyright expires 50 years after the work is made available to the public with the consent of the copyright owner or after the work is first published, or if the work is not so made available to the public or published within 50 years of its making, then copyright expires 50 years after the making of the work (s 3(2)(b)). Sound recordings and published editions enjoy protection for 50 years from the date on which they are first published (s 3(2)(c) and (f)), and broadcasts and programme-carrying signals enjoy protection for a period of 50 years after they are made (s 3(2)(d) and (e)).

Unfortunately, it seems as if boundaries are shifted by the adaptation of copyright law to the demands of the digital environment, which shift erodes the public domain.<sup>18</sup> This can be ascribed partly to the protection of technological protection measures which allow authors to lock up works or ideas that should flow freely within the public domain. The protection of these measures may potentially nullify the doctrine of exhaustion – by protecting access control, for example, authors can charge again and again for each individual access.<sup>19</sup>

Stronger copyright protection has affected not only the public domain but also the private domain. Traditional copyright principles provide for a number of exceptions and limitations to authors' exclusive rights to enable users to use copyright works within the parameters set by law. The expansion of copyright protection, the granting of new exclusive rights, and the creation of new forms of infringement enable authors to maximize their profits from the digital exploitation of their works. Unfortunately, international experience has shown, as I indicated earlier, that the copyright limitations and exceptions have not been reworked to ensure that user privileges are not curtailed in the digital environment.<sup>20</sup>

### **6.3 Copyright Protection, Human Rights, and Developing Countries**

Intellectual property rights are entrenched as human rights in the Universal Declaration on Human Rights (UDHR).<sup>21</sup> Article 27.2 states that '[e]veryone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author'. So intellectual property rights are as such treated as an integral part of the human rights spectrum.

Other human rights are inextricably intertwined with intellectual property rights. These rights include the right to development, the right to education, and the right to freedom of expression.

---

<sup>18</sup> Sun op cit note 2 at 202-203.

<sup>19</sup> Idem at 204.

<sup>20</sup> Idem at 205.

<sup>21</sup> 'Universal Declaration of Human Rights, Adopted and proclaimed by General Assembly resolution 217 A (III) of 10 December 1948' accessible at <<http://www.un.org/Overview/rights.html>> (last visited on 14 February 2006).

The right to development is contained in article 27.1 of the UDHR: 'Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits.' Article 26.1, in turn, provides for the right to education:

'Everyone has the right to education. Education shall be free, at least in the elementary and fundamental stages. Elementary education shall be compulsory. Technical and professional education shall be made generally available and higher education shall be equally accessible to all on the basis of merit.'

The right to freedom of expression is stated in article 19: 'Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.'

One would have thought that the ease of digital transmission and the global accessibility of information would have brought these human rights closer to manifestation in developing countries. One would have been wrong. Truth is that stronger copyright protection has shrunk the public domain and narrowed copyright exceptions and limitations. This has increased the cost of operating education systems and sharing information between developed and developing countries.

Also, the laws against the circumvention of technological protection measures, the extension of copyright terms, and the protection of non-original databases have seriously curtailed freedom of expression. If these rules were to be introduced in developing countries, they would widen the digital divide and hamper the realization of the above human rights.<sup>22</sup>

#### **6.4 Current South African Legislation**

Currently South Africa has no legislation specifically regulating the protection of digitized copyright works. I shall now analyse the relevant sections of the Constitution of the Republic of

---

<sup>22</sup> Sun op cit note 2 at 210.

South Africa, 1996,<sup>23</sup> the Copyright Act,<sup>24</sup> and the Electronic Communications and Transactions Act.<sup>25</sup>

#### **6.4.1 The Constitution of the Republic of South Africa**

The Constitution of the Republic of South Africa, 1996 was certified by the Constitutional Court on 4 December 1996 and took effect on 4 February 1997.

Chapter 3 of the Constitution contains the Bill of Rights. Only three provisions of the Bill of Rights are relevant for present purposes: section 25 on the right to property, section 16 on freedom of expression, section 29 on the right to education, and section 32 on access to information. The right to property safeguards the rights of the author, whereas the latter three rights impact on user privileges (I shall deal with them elsewhere).<sup>26</sup>

Section 25 of the Constitution states: ‘No one may be deprived of property except in terms of law of general application, and no law may permit arbitrary deprivation of property.’ The term ‘property’ includes intellectual property.<sup>27</sup> So an author’s exclusive rights are protected by the Constitution as property.

However, the right to property, as well as the rights to freedom of expression, education, and access to information (like all other rights entrenched in the Bill of Rights) are not absolute but subject to possible limitation. Section 7(3) of the Constitution provides that the rights in the bill of rights are subject to the limitations contained in section 36. Section 36 states:

‘The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society

---

<sup>23</sup> Act 108 of 1996 (‘the Constitution’).

<sup>24</sup> Op cit note 15.

<sup>25</sup> Act 25 of 2002 (‘the ECT Act’).

<sup>26</sup> I shall refer to these provisions in Chapter 7 on the emergence of an access right.

<sup>27</sup> See *Ex parte Chairperson of the Constitutional Assembly: In re Certification of the Constitution of the Republic of South Africa, 1996* 1996 (4) SA 744 (CC).

based on human dignity, equality and freedom, taking into account all relevant factors, including –

- (a) the nature of the right;
- (b) the importance of the purpose of the limitation;
- (c) the nature and extent of the limitation;
- (d) the relation between the limitation and its purpose; and
- (e) less restrictive means to achieve the purpose.’

To be justifiable under the limitation clause, a limitation of rights must be authorized by law of general application. The term ‘law’ includes legislation, common law, or customary law.<sup>28</sup> Where an administrative official must determine the limitation,<sup>29</sup> or where rights are limited without resorting to the law,<sup>30</sup> the limitation will fail to qualify as a law of general application, and the resulting limitation of rights will be unconstitutional.

The limitation of rights involves a weighing up of competing social and ethical values. Different rights have different implications for democracy. The following considerations must be taken into account when balancing competing interests: the nature of the right that has to be limited and its importance for an open and democratic society based on freedom and equality; the purpose for which the right is being restricted and the significance of that purpose to such a society; the extent of the limitation; and whether the desired result could not reasonably be achieved by other means less deleterious to the right in question.<sup>31</sup>

Certain rights will emerge as more important than others. In *S v Makwanyane*,<sup>32</sup> the rights to life and human dignity have already emerged as the most important of all human rights, but it remains to be seen which hierarchy of the remaining rights the courts will develop.

---

<sup>28</sup> See, for example, *Khala v Minister of Safety & Security* 1994 (4) SA 218 (W) 227G: ‘In my view, the rules relating to the claim of privilege by the State in respect of a police docket is a “law of general application”’.

<sup>29</sup> *Dawoo v Minister of Home Affairs, Shalabi v Minister of Home Affairs, Thomas v Minister of Home Affairs* (CC); 2000 (3) SA 936 (CC).

<sup>30</sup> *August v Electoral Commission* 1999 (3) SA 1 (CC).

<sup>31</sup> GE Devenish ‘Constitutional Law’ in *LAWSA* vol 5(3) 2 ed (2004) para 160 at 184-185.

<sup>32</sup> 1995 (3) SA 391 (CC).

From the above it is clear that either the author's right to intellectual property or the user's right to freedom of expression, education, and access to information may be limited if done so by a law of general application, and if such limitation meets the criteria set out in section 36. This will especially be important when considering the claims of authors to protection against circumvention and the claims of users to exceptions and limitations. Such consideration will involve a weighing up of the conflicting rights of the authors and the users.

## **6.4.2 The Copyright Act**

The Copyright Act creates two forms of copyright infringement – direct and indirect infringement. Also, certain acts of infringement give rise to criminal liability. As the provisions relating to indirect infringement<sup>33</sup> and criminal liability<sup>34</sup> relate to dealings with infringing copies, they are by their nature not relevant to this discussion.

### **6.4.2.1 Direct Infringement**

Direct infringement takes place when a person, without the authority of the author, does or causes someone else to do any of the acts that are, in respect of that type of copyright work, designated as restricted acts and so within the exclusive domain of the author.<sup>35</sup>

Direct infringement, then, takes two forms – where a person, without the authority of the author, performs any of the restricted acts, and where a person, without authority of the author, causes someone else to perform any of the restricted acts.

Van Coppenhagen<sup>36</sup> argues that, in order to preserve the copyright balance, an anti-circumvention prohibition should be subject to an infringement criterion – a requirement that the

---

<sup>33</sup> Section 23(2) and (3) of the Copyright Act.

<sup>34</sup> Section 27(1) of the Copyright Act.

<sup>35</sup> Section 23(1) of the Copyright Act.

<sup>36</sup> Vanessa van Coppenhagen 'Copyright and the WIPO Copyright Treaty, with Specific Reference to the Rights Available in a Digital Environment and the Protection of Technological Measures' (2002) 119 *South African Law Journal* 429 at 445.

result of circumvention should be copyright infringement. If this were to be done, then a prohibition against the act of circumventing a technological protection measure for unlawful purposes would add nothing to the existing law, inasmuch as the author, in any event, has an action for copyright infringement against the person who does any of the restricted acts. This argument goes against the international trend, however, which, as I have shown, is to treat the act of circumvention separately from the act of direct infringement.

Van Coppenhagen<sup>37</sup> also argues that the making available of a device that enables a person to circumvent a technological protection measure for the purposes of infringing copyright may constitute an infringement covered by the phrase ‘causes someone else to do’ in section 23(1). This argument is artificial and loses sight of the legislative intent of inserting the phrase in section 23(1) – it is a legislative affirmation of liability for the unlawful conduct of others on the basis of the maxim *qui facit per alium facit per se*. A person who traffics in circumvention devices, which may be used for lawful and unlawful purposes, in no way ‘causes’ the direct infringement performed by someone who uses such a device for (unlawful) infringing purposes, in the same way that a person who sells steak knives in no way ‘causes’ the death of someone stabbed with one of these knives.

To conclude: nothing in the Copyright Act can be construed as the legislative basis of liability for the circumvention of technological protection measures.

#### **6.4.2.2 Contributory Liability**

In all types of unlawful action, liability is imposed not only on those who directly commit the delict, but also on those who assist, aid, or abet the commission of a delict.<sup>38</sup> It is clear that copyright is not only infringed by the actual perpetrator of an infringing act but also by someone who instigates or instructs the doing of that act, or assist in the doing of the infringing act.<sup>39</sup> The instigator of the infringing act commits contributory copyright infringement.<sup>40</sup>

---

<sup>37</sup> *Idem* at 450.

<sup>38</sup> *McKenzie v Van der Merwe* 1917 AD 41 at 51.

<sup>39</sup> *Atari Inc & another v JB Radio Parts (Pty) Ltd* (TPD (case no 17419/83) unreported); *Bosal Africa (Pty) Ltd v*

The remedies available to a successful plaintiff in an action for contributory infringement are damages and an interdict. Fault is required in respect of an award of damages only. This principle is in line with article 45.1 of the TRIPS Agreement, which requires that 'judicial authorities shall have the authority to order the infringer to pay the right holder damages adequate to compensate for the injury the right holder has suffered because of an infringement of that person's intellectual property right by an infringer who knowingly, or with reasonable grounds to know, engaged in infringing activity'.<sup>41</sup>

Where infringement results from the circumvention of a technological protection measure, the person who made the circumvention device available to the infringer assisted, aided, or abetted copyright infringement, and could thus be held liable for contributory copyright infringement. Damages would be awarded only where the person who made the device available knew, or had reasonable grounds to know, that the device will be used for infringement purposes.

In terms of South African law, a person who trafficks in circumvention devices could thus be held liable for contributory copyright infringement.

### **6.4.3 The Electronic Communications and Transactions Act**

The Electronic Communications and Transaction Act (the ECT) came into operation on 30 August 2002.<sup>42</sup> Chapter XIII of the ECT deals with cyber crime.<sup>43</sup>

Section 86 of the ECT Act protects 'data'. In terms of section 1, the term 'data' 'means electronic representations of information in any form'. A copyright work in digital form is

---

*Grapnel (Pty) Ltd & another* 1985 (4) SA 882 (C).

<sup>40</sup> See further Coenraad Visser 'Online Service Provider Liability Under the Electronic Communications and Transactions Act 25 of 2002' (2002) 14 *South African Mercantile Law Journal* 758 at 759.

<sup>41</sup> *Ibid.*

<sup>42</sup> Proc R68 GG 23809.

<sup>43</sup> For a brief discussion of this chapter, see Dana van der Merwe 'Computer Crime – Recent National and International Developments' (2003) 66 *Tydskrif vir Hedendaagse Romeins Hollandse Reg* 30 at 43-44.

nothing but an electronic representation of information, and so the definition of data is broad enough to include digital copyright works.

Section 86 creates only criminal offences<sup>44</sup> and does not impose civil liability.

Section 86(1) creates an access offence: ‘Any person who intentionally and unlawfully accesses or intercepts any data without authority or permission to do so, shall be guilty of an offence.’

Section 86(3) states:

‘A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilize such item to contravene this section, is guilty of an offence.’

Note that section 86(3) contains a requirement that a prohibited device must have been designed *primarily* to overcome security measures or access codes. Note also the breadth of the prohibition – the mere possession of a designated device is sufficient to found criminal liability.

Finally, section 86(4) provides:

‘A person who utilises any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, is guilty of an offence.’

---

<sup>44</sup> The sanctions are stipulated in section 89 of the ECT Act.

Subsections (1) and (4) of section 86 of the ECT Act concern the act of unlawful access to protected data, whereas subsection (3) concerns the trafficking in devices primarily designed to obtain such unlawful access. In both instances intent is required.

Given that digital copyright works fall within the ambit of 'data', section 86 creates criminal liability for both the act of circumventing technological protection measures, and for trafficking in circumvention devices. It is interesting to note that, like the corresponding provisions introduced by the DMCA, the proscribed act of circumvention is limited to the circumvention of access control, whereas the prohibition on circumvention devices extends to devices circumventing access control and to security devices (copy control).

The unlawfulness requirement in the section 86 prohibitions relates to the absence of a suitable end-user exception or limitation legitimizing the user's circumventing conduct, or the absence of the author's consent to access. No such exception or limitation is provided in the ECT Act. Given the independence of the act of circumvention and any subsequent act of copyright infringement, the end-user exceptions in the Copyright Act<sup>45</sup> would be of no avail to an accused under the ECT Act. This means that the protection against the circumvention of technological protection measures in South Africa is far stricter than such protection in the United States and Europe.

This is also where the Constitution enters the picture again. Under certain circumstances the provisions of section 86 of the ECT Act could curtail users' privileges in such a way that it would impact on their rights of freedom of expression, education and access to information. Would such a limitation on users' rights be in accordance with the provisions of the limitation clause in the bill of rights?

The inquiry should be done in two stages. In the first instance, we should determine whether there has been an infringement of user rights. If this is found to be the position, we should then

---

<sup>45</sup> Such as section 12 of the Copyright Act.

decide whether or not the infringement is valid in terms of the criteria for the limitation of rights as set out in section 36 of the South African Constitution.<sup>46</sup>

Where the provisions of section 86 of the ECT Act limit user privileges by curtailing their rights of freedom of expression, education, and access to information, it is clear that there would be an infringement of rights.

Secondly, one should determine whether this limitation of the human rights of users would be valid in terms of the criteria set out in section 36 of the Constitution. The first requirement set out by section 36 is that the limitation should be in terms of law of general application. Section 86 of the ECT Act meets this requirement. The next step would involve the balancing of the competing interests of the authors and the users. I have already referred to the considerations that have to be taken into account when balancing competing interests. It would be up to courts to decide which of the competing interests would be the most important for an open and democratic society based on freedom and equality. Taking South Africa's status as developing country into consideration, it would seem as if user's rights may well outweigh author's rights.

If this would be the case, section 86 would be unconstitutional as an unreasonable limitation of the relevant human rights of users.

## **6.5 A possible South Africa-United States Free Trade Agreement?**

In June 2003 the United States opened negotiations with the Southern African Customs Union (SACU) in order to conclude a Free Trade Agreement (FTA).<sup>47</sup> In March 2006, the negotiations collapsed.<sup>48</sup> There were two main reasons for the collapse. In the first instance, SACU is structurally not yet able to take joint negotiating positions outside of tariffs in goods and

---

<sup>46</sup> *S v Makwanyane* supra note 32. However, in *Christian Education South Africa v Minister of Education* 2000 (4) SA 757 (CC), the Constitutional Court demonstrated that it was willing to depart from the two-stage approach to rights and their limitation in order to avoid the difficulty of deciding whether a right was indeed infringed (see GE Devenish op cit note 31 par 163 at 186-187).

<sup>47</sup> Formed in 1889, SACU is the world's oldest trading bloc. It comprises Botswana, Lesotho, Namibia, South Africa, and Swaziland.

<sup>48</sup> See <<http://www.tralac.org/scripts/content.php?id=4774>> (visited on 28 June 2006).

agriculture (its competence is restricted by the SACU Agreement).<sup>49</sup> The United States FTA template included topics like trade in services, investment, and competition. Secondly, the United States is faced with the expiry of the President's 'trade promotion authority', which allows the executive to fast track trade deals through Congress.<sup>50</sup>

After calling off these negotiations, the United States indicated its intention to negotiate new trade arrangements with several African countries, such as Kenya, Mauritius, Mozambique, and Ghana.<sup>51</sup>

When one looks at the FTA that the United States concluded with Australia,<sup>52</sup> for example, it is clear that the United States imposes on its FTA partners an obligation to implement provisions along the lines of those devised by the DMCA to safeguard technological protection measures against circumvention.

As I have shown, by virtue of the ECT Act and its silence as to user exceptions and limitations, authors in South Africa enjoy stronger protection than their United States counterparts. So it is ironic that if South Africa were to be forced by a FTA to adopt DMCA-like anti-circumvention provisions, users would be in a better position than they are now, and the copyright balance may be corrected.

## 6.6 Conclusion

A net exporter of copyright works would arguably opt for strong copyright protection in order to obtain greater economic benefit from the royalties earned by these works in terms of trade. So it

---

<sup>49</sup> Articles 38-39 of the SACU Treaty make provision for Member States to develop common policies and strategies only with respect to industrial development and agriculture: see The Customs Union Agreement between South Africa, Botswana, Lesotho, Namibia and Swaziland of 21 October 2002 (which entered into force 15 July 2004). Full text available at

<[eprints.unimelb.edu.au/archive/00001628/01/wholeMutai\\_.pdf](http://eprints.unimelb.edu.au/archive/00001628/01/wholeMutai_.pdf)> (visited on 29 January 2007).

<sup>50</sup> See <<http://www.tralac.org/scripts/content.php?id=4774>> op cit note 48.

<sup>51</sup> See <<http://www.nationmedia.com/eastafrican/current/News/News2606200619.htm>> (visited on 28 June 2006)

<sup>52</sup> The Australia-United States Free Trade Agreement op cit note 10 entered into force on 1 January 2005. Article 17.1.4 obliges Australia to ratify the WCT and the WPPT, whereas article 17.4.7 basically reiterates the anti-

follows that the United States and the European Union should prefer strong copyright protection, including strong protection against the circumvention of technological protection measures, in order to generate trade revenue from the export of the works of their authors.<sup>53</sup> By contrast, a net importer of copyright works, like South Africa, should arguably opt for weaker copyright protection, as this would result in less money leaving the country as royalties for foreign authors.<sup>54</sup>

Van Coppenhagen,<sup>55</sup> however, argues that South Africa would benefit from the implementation of the anti-circumvention prohibition: 'For a developing country such as South Africa, which finds itself in a global information economy, the core of which is creativity and its dissemination, intellectual property protection, and particularly copyright protection, is vital.' This argument flies in the face of economic and social reality, of course.

Unfortunately, as I have shown, South Africa has, inadvertently perhaps, adopted anti-circumvention provisions that are far stricter than those adopted in developed countries such as the United States and those of the European Union. To the extent that the South African prohibitions in the ECT Act may fall foul of the constitutional protection of certain human rights, they may well be unconstitutional. In Chapter 8, I shall propose legislative language that may restore the copyright, and constitutional, balance.

---

circumvention provisions of the Digital Millennium Copyright Act (DMCA).

<sup>53</sup> Selena Kim 'The Reinforcement of International Copyright for the Digital Age' (2002) 16 *Intellectual Property Journal* 93-122 at 107-108.

<sup>54</sup> *Ibid.*

<sup>55</sup> Van Coppenhagen *op cit* note 36 at 430.

## CHAPTER 7: THE EMERGENCE OF AN ACCESS RIGHT

‘Alice opened the door and found that it led into a small passage, not much larger than a rat-hole: she knelt down and looked along the passage into the loveliest garden you ever saw. How she longed to get out of that dark hall, and wander among those beds of bright flowers and those cool fountains, but she could not even get her head through the doorway.’

LEWIS CARROL

*Alice’s Adventures in Wonderland*

### 7.1 Introduction

Why should one concern oneself with whether the protection of technological protection measures creates a new exclusive access right? The answer is simple – in the digital environment, without access there cannot be any use. The person who controls access to a work also controls the use of that work. Ginsberg<sup>1</sup> states that ‘because “access” is a prerequisite to “use”, by controlling the former, the copyright owner may well end up preventing or conditioning the latter’. So the access right will arguably become the most important right of an author in the digital world.

But what, exactly, is access? Quite simply, it is the ability to experience or apprehend a work; put differently, it is the ability to view, read, or listen to a work.<sup>2</sup>

In an attempt to answer the question whether the prohibition on the circumvention of technological protection measures indeed created an exclusive access right, I shall examine the following questions: What is the difference between access in the analogue world and access in the digital world? Did an exclusive access right exist in the analogue world? I shall then explore not only the provisions of the WIPO Copyright Treaty but also of different

---

<sup>1</sup> Jane C Ginsberg ‘Copyright Legislation for the “Digital Millennium”’ (1999) 23 *Columbia-VLA Journal of Law & the Arts* 137 at 143. See also Christine Jeanneret ‘The Digital Millennium Copyright Act: Preserving the Traditional Copyright Balance’ (2001) 12 *Fordham Intellectual Property, Media and Entertainment Law Journal* 157 at 175; Kamiel J Koelman ‘The protection of technological measures vs. the copyright limitations’ paper presented at the *ALAI Congress Adjuncts and Alternatives for Copyright*, New York, 15 June 2001 accessible at <<http://www.ivir.nl/publications/koelman/alaiNY.html>>.

<sup>2</sup> June M Besek ‘Anti-Circumvention Laws and Copyright: A Report from the Kernochan Center for Law, Media and the Arts’ (2004) 27 *Columbia Journal of Law & the Arts* 385 at 474.

national laws to determine whether an access right has been recognized in the digital world. Lastly, I shall examine the effect on users of copyright works of the recognition of an access right, as well as the question as to whether users in the digital world now have a corresponding right to demand access.

## **7.2 Access in the Analogue World and Access in the Digital World**

Analogue works are typically embodied in physical objects such as books. The work protected by copyright and the physical object embodying the work are inseparable, which gives the person in possession of the physical object the right to control access to the embedded copyright work. Mere physical possession is sufficient for purposes of access control – ownership is not a requirement.

The only control that authors have over access to their analogue works is the limited control that they have over access to the physical copies of their works. So they can control access to their works only as long as they control the physical objects embodying their works. This principle is recognized in copyright law in the distribution and public communication exclusive rights granted to authors. (The distribution right connotes the right of an author to make his or her work available to the public for purchase if he or she so chooses.<sup>3</sup> The traditional right of communicating a work to the public refers to the right of an author to control and condition access to her work by charging the public for such access (for example, an admission fee to a film).)

So in the analogue world, users can gain access to any copyright work merely by being in possession of the physical embodiment of such work. Nothing more is required.

All of this changed in the 1980s with the advent of satellite transmission. Transmissions and signals are not embodied in physical, tangible objects. This means that these two types of work exist separate and distinct from physical objects.<sup>4</sup> Possession of a physical object was no longer a prerequisite for access to the transmission or signal – these works could be accessed without physical possession. The only requirement for access was a device that

---

<sup>3</sup> *Harper & Row Publishers Inc v Nation Enterprises* 471 US 539 (1985).

<sup>4</sup> Even though the signals and transmissions are intangible, they have to be received and played back on devices

could translate the intangible signals and transmissions into a form susceptible to the human senses in order to experience the work. Access, then, was no longer limited to those who had physical possession of the objects embodying the protected works. Even those without such physical possession could intercept and access these works on playback devices.

Unauthorized access now became a reality. And it is also unauthorised access, and not unauthorized copying, that became the main threat to the rights of authors.<sup>5</sup>

The separation of works from the physical objects embodying them did not stop with transmissions and signals. Digitization made it possible to dematerialize any type of work into electronic or digital format. So potentially any work can now exist separate and distinct from a physical object. A consequence of the separation of a work and the object containing that work is that possession is no longer required for access. So authors can no longer control access merely by physically controlling the distribution and communication to the public of their works, and users can access works without being in possession of the physical embodiment of the work (the Internet is a good example of this type of access).

The dematerialization of works into digital format revolutionized the ways in which access to copyright works is controlled. The digital world, therefore, demanded new measures that would enable authors to control access to their works. In this new world, authors use their own protection measures (such as contracts, and technological protection measures (specifically access controls)) in an attempt to regulate access to their works.

Ginsberg<sup>6</sup> identifies two types of access control – the measure controlling ‘access to a work’ and the measure controlling ‘access to *a copy of the work*’.<sup>7</sup> She<sup>8</sup> uses the following example to illustrate this distinction:

‘Suppose I purchase a CD ROM containing a copyrighted work, such as a video game. Suppose also to view and play the game, I must register with the producer, using the modem in my computer. The computer in turn communicates a password to

---

to make them susceptible to the human senses.

<sup>5</sup> Jonathan Weinberg ‘Digital TV, Copy Control, and Public Policy’ (2002) 20 *Cardozo Arts and Entertainment Law Journal* 277 at 281.

<sup>6</sup> Ginsberg op cit note 1 at 140.

<sup>7</sup> The measure controlling ‘access to a work’ is a new right introduced in the Digital Millennium Copyright Act (DMCA).

me. A technological measure included in the CD ROM recognizes my password, and my computer. Thenceforth, each time I want to play the game, I must enter my password, and play the game on the same computer. This means that I cannot use that copy of the game on another computer. It also may mean, at least in theory, that I cannot communicate my password to a friend or family member to play the game on my computer, since the password protects access to the work, and my disclosure of the password is an act that circumvents a protective measure.’

In this scenario, the user gains lawful access to *a copy of the work* by purchasing the CD ROM. But she does not access *the work* until she keys in the password. A person may lawfully acquire a copy of work (such as a CD ROM) but still not obtain access to the work (the embedded video game) except by following the procedure dictated by the author.

If the law prohibits circumvention of controls to access a *work*, a person would not be able to circumvent the access controls, even for lawful purposes. Accordingly, where the law bars the circumvention of access controls to the *work*, access is a repeated action, and hence each access could constitute circumvention. So the user cannot give her password to her friend, as she would be circumventing the access control. However, if the law bars the circumvention of technological measures controlling access to *a copy of a work*, then once she lawfully acquired her copy, she would be able to use it without any further prohibitions imposed by law; she would, in American copyright parlance, be allowed to make fair use of the embedded protected work.<sup>9</sup>

In *Lexmark International Inc v Static Control Components Inc*,<sup>10</sup> the United States District Court likewise appreciated the distinction between copies of works, on the one hand, and the works, on the other. The court distinguished between ‘copies of works (such as books, CD’s and motion pictures) that have an independent market value’ and ‘a work protected under’ the Copyright Act.

So ‘access to a copy of a work’ would entail access to the physical embodiment of the protected work. ‘Access’, in this sense, would resemble the traditional copyright concepts

---

<sup>8</sup> Ginsberg op cit note 1 at 140.

<sup>9</sup> Idem at 140-141.

inherent in the exclusive rights of distribution and communication to the public. From an author's perspective, this type of access entails making a work accessible to the public at large. It also has an impersonal element – the author will not necessarily know the identity of the user accessing the work.

'Access to a work', then, differs from 'access to a copy of a work' in the sense that access to a work does not depend on access to the physical embodiment of the work. This type of access is made available to an individual, not to the public. It is also personal – the author will usually have an indication of the identity of the user. So Ficsor's<sup>11</sup> comment that the personal use of the user is not relevant is not true in the digital environment – digital access is actually specifically aimed at individual access. Ginsberg<sup>12</sup> identifies a further distinction – in the digital context every subsequent access to a work can be controlled, while the traditional rights to control access to a copy of a work (the distribution and communication rights) do not constrain the purchaser's further disposition of that copy.

### **7.3 An Exclusive Access Right in the Analogue Environment?**

Does copyright legislation acknowledge access control as an exclusive right with regards to analogue works?

Writers such as Jeanneret<sup>13</sup> believe that an access right is indeed recognized in the analogue environment. Authors have traditionally controlled and conditioned access to their works by charging the public for such access (for example, an admission fee to a movie). So the access right is already recognized in the form of the author's distribution and communication rights. Ficsor<sup>14</sup> agrees with this argument. According to him, two acts are interwoven inseparably at the moment of getting access – the first is the act of making the work available, and the second, the personal use of the work. Only the act of making the work available by distributing or communicating it involves the exercise by the author of her rights. Ficsor

---

<sup>10</sup> 253 F Supp 2d 943 (ED Ky 2003) at 969.

<sup>11</sup> Mihály Ficsor *The Law of Copyright and the Internet: The 1996 WIPO Treaties, Their Interpretation and Implementation* (2002) at 551 C11.15.

<sup>12</sup> Jane C Ginsberg 'From Having Copies to Experiencing Works: the Development of an Access Right in U.S. Copyright Law' in Hugh Hansen (ed) *U.S. Intellectual Property: Law and Policy* (2000), cited by Jeanneret op cit note 1 at 191.

<sup>13</sup> Jeanneret op cit note 1 at 190.

<sup>14</sup> Ficsor op cit note 11 at 551 C11.15.

equates access to breaking the lock of a closed shop, taking a CD, and walking out without payment.<sup>15</sup> He argues that the second act (the personal use of the work) is not relevant to copyright law.

What these writers fail to recognize is that even though analogue copyright was always concerned with access,<sup>16</sup> it never recognized access as such as an exclusive right. Analogue access control was a mere consequence of physical possession and so access control is not listed in any copyright legislation from the analogue era as an exclusive right. Instead, it is recognized only indirectly by the rights of distribution and communication to the public.

#### **7.4 An Exclusive Access Right in the Digital Environment?**

As I have indicated, there are two types of technological protection measure – access control, and copy control. As copyright legislation worldwide expressly recognize the right of authors to control the uses of their works, the protection of copy control adds no new right to the existing bundle of exclusive rights extended to authors.

But it is clear that access in the analogue world is different from access in the digital world. It is also clear that copyright legislation in the analogue world does not expressly recognize access control as such as an exclusive right. This begs the question, of course, as to whether the protection of access control to digital works creates a *right* to control access in the digital environment. Does the fact that the law now protects access control imply that it indirectly recognizes a right to control digital access and so adds a new right to the author's bundle of rights?

I shall now examine the provisions of the WCT and of implementing legislation in several jurisdictions in an attempt to determine whether, in the digital environment, the protection of access controls against circumvention indeed creates an access right.

---

<sup>15</sup> The United States legislator, while drafting the DMCA, used a similar comparison: it likened circumventing an access controlling measure to breaking into a locked room to steal a copy of a book (US House of Representatives, WIPO Copyright Treaties Implementation and On-Line Copyright Infringement Liability Limitation, Report to Accompany H.R. 2281, 22 May 1998, Report 105-551, pt 1, p 19, cited by Kamiel J. Koelman 'A Hard Nut to Crack: The Protection of Technological Measures' [2000] *European Intellectual Property Review* 272 at 276n33.

<sup>16</sup> Jonathan Griffiths & Uma Suthersanen (eds) *Copyright and Free Speech Comparative and International Analyses* (2006) in para 12.33 at 303 and para 12.35 at 304.

## 7.5 The Emergence of an Access Right

### 7.5.1 The WIPO Copyright Treaty

The WCT extends the existing rights under the Berne Convention in two ways – directly by establishing the distribution,<sup>17</sup> rental,<sup>18</sup> and communication to the public<sup>19</sup> rights, and indirectly by creating two additional types of infringement – the circumvention of technological protection measures,<sup>20</sup> and the removal or alteration of rights management information.<sup>21</sup> Only the circumvention of technological protection measures concerns me here.

The WCT does not directly create an exclusive access right. For purposes of the present discussion, I shall briefly refer to the WCT's distribution and communication rights to determine whether these two rights perhaps encompass an access right. I shall then refer to the prohibition on circumvention to establish whether this prohibition indirectly creates an access right.

Article 6 of the WCT deals with the distribution right. Article 6.1 states that the 'authors of literary and artistic works shall enjoy the exclusive right of authorizing the making available to the public of the original and copies of their works through sale or other transfer of ownership'. Article 6.2 leaves it to the Contracting Parties to determine the conditions, if any, under which the doctrine of exhaustion will apply.

Article 6 of the WCT extends the right of distribution to all categories of works, even though it uses the seemingly limiting phrase 'literary and artistic works'.<sup>22</sup>

---

<sup>17</sup> Article 6 of the WCT.

<sup>18</sup> Article 7 of the WCT.

<sup>19</sup> Article 8 of the WCT.

<sup>20</sup> Article 11 of the WCT.

<sup>21</sup> Article 12 of the WCT.

<sup>22</sup> Article 1.1 of the WCT makes it clear that the WCT is a special agreement within the meaning of article 20 of the Berne Convention, and article 1.4 obliges contracting parties to comply with articles 1 to 21 and the Appendix of the Berne Convention. Furthermore, in terms of article 3 of the WCT, contracting parties are obliged to apply the provisions of articles 2 to 6 of the Berne Convention. Article 2(1) of the Berne Convention defines 'literary and artistic works' very broadly, to include 'every production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression ...'. From this definition as well as the

The Agreed Statement on Articles 6 and 7 expressly states that the right of distribution refers ‘exclusively to *fixed* copies that can be put into circulation as *tangible objects*’ (emphasis added). So the distribution right confers a right to control access to a physical *embodiment*, rather than a right to control access to an embedded *work*.

Article 8 of the WCT synthesizes the various provisions of the Berne Convention relating to public performance into a general right of ‘communication to the public’. It provides that ‘authors . . . shall enjoy the exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them’.

It is clear from the concluding phrase of article 8 that communication to the public includes interactive, digital delivery. This right appears to cover ‘access’ to a work through online media, but it is less clear whether it also extends to subsequent access to the work once the user has downloaded the work, or acquired a free-standing copy, such as a CD-ROM.<sup>23</sup> Van Copenhagen<sup>24</sup> believes that article 8 grants the author the exclusive right to *provide* access, and not the exclusive access right. So it seems as if this right covers only the right to provide initial access to online media. The right to communicate a work to the public, then, seems like a digital online equivalent of the analogue publication right.

As the WCT does not directly create an access right, the question arises as to whether it does not perhaps indirectly create such a right. Article 11 of the WCT introduces the obligation to protect technological protection measures employed by authors. Two interpretations of this article have been offered – it *indirectly* creates a new right of access, or it excludes access control technologies from protection and so does not create an access right (not even indirectly).

---

examples given, it is clear that the expression ‘literary and artistic works’ encompasses all categories of works. Thus, whenever the WCT refers to ‘literary and artistic works’ it includes all categories of works because of its special relationship with the Berne Convention.

<sup>23</sup> Ginsberg op cit note 1 at 142.

<sup>24</sup> Vanessa van Copenhagen ‘Copyright and the WIPO Copyright Treaty, with Specific Reference to the Rights Applicable in a Digital Environment and the Protection of Technological Measures’ (2002) 119 *South African*

On the one hand, it is argued that article 11 *indirectly* creates an access right. Although an access right does not fall within the range of an author's exclusive rights, proponents of this argument believe that it is generally accepted<sup>25</sup> that the 'technological protection measures' referred to in article 11 includes access and copy control technologies, from which flows that it was not necessary expressly to refer to access controls. Article 11, therefore, protects access controls. And since it protects access control technologies, it indirectly recognizes a right of access.

On the other hand, one can argue that the WCT is silent on the control of access to a work. Article 11 expressly states that the only technological protection measures that are protected are those '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'. Article 11, therefore, protects only those technological protection measures that protect the traditional exclusive rights granted by the Berne Convention, and the distribution and communication to the public rights granted by the WCT. Accordingly, it protects only copy controls. Since neither the Berne Convention nor the WCT expressly provides for an access right,<sup>26</sup> it is clear that access controls are not protected by article 11.

I believe that the argument favouring the protection of access controls is flawed. In the first instance, article 11 does not expressly refer to access controls – it refers only to those measures that protect existing rights under the Berne Convention and the WCT. To argue that such measures include access controls runs counter to the explicit language of the WCT. Secondly, if it is true that the WCT creates an access right (which never before existed in copyright law), one would have expected such a right to be created expressly by the WCT.<sup>27</sup> To me it seems as if the language of the WCT does not justify a conclusion that it creates a new access right.

Although it seems as if the Treaty itself did not create an exclusive access right, it does seem

---

*Law Journal* 429 at 452.

<sup>25</sup> See, inter alia, <<http://www.ifpi.org/site-content/library/wipo%20treaties%20-%20technical%20measures.pdf>> (visited on 5 April 2002) as well as the DMCA.

<sup>26</sup> Jonathan Band & Taro Isshiki 'Digital Copyright Law - US: The New US Anti-Circumvention Provision: Heading in the Wrong Direction' (1999) 15 *Computer Law & Security Report* 219 at 225.

<sup>27</sup> Van Coppenhagen op cit note 24 at 443.

as if national legislators interpret the Treaty provisions in such a way so as to make provision indeed for an exclusive access right. Actually, in several jurisdictions a right to control access *to information* was already recognized before the adoption of the WCT. In most of these legislative implementing provisions, the ‘access’ measures directly protect information, while the provisions implementing the WCT indirectly protect access by protecting technology which, in turn, protects works.

I shall examine the position in three jurisdictions – the United States, the European Union, and South Africa. It seems as if the international trend is to recognize two closely related rights – a general right to control access to information or information services, and a more specific right to control access to works protected by copyright. For present purposes, I shall refer only to the right to control access to works protected by copyright.

### **7.5.2 The United States of America**

In several federal laws the United States recognized a right to control access to information.<sup>28</sup>

There is also further Federal statutes that prevent access in an effort to maintain the integrity of either certain devices, or to protect certain information. These statutory measures include regulations governing fraud in connection with access devices.<sup>29</sup> Federal ‘breaking and entering’ statutes<sup>30</sup> render forced access a crime.<sup>31</sup> Many state laws address the unauthorized access to information and/or protection and privacy measures.<sup>32</sup>

The right to control access to a work protected by copyright was never recognized as one of an author’s exclusive rights. No access control technology could, therefore, be protected by a provision that protects a system that protects ‘a right of the copyright owner’. It also seems as

---

<sup>28</sup> 18 USC § 1030 (the Computer Fraud and Abuse Act); 18 USC § 2511(1) (the Electronic Communications Privacy Act); 18 USC § 2701 (the Stored Wire and Electronic Communications Act); 47 USC §§ 605(a) and (e)(3) and (4) (the Communications Act); art 1707 of The North American Free Trade Agreement (NAFTA) 32 ILM 605.

<sup>29</sup> 18 USC § 1029 (2003) (criminalizing the act of one who, with ‘(a)(2) intent to defraud ... traffics in or uses ... an unauthorized access device ... [or] (a)(7) uses, produces, ... or possesses a telecommunications instrument ... modified or altered to obtain unauthorized use of telecommunications services’.

<sup>30</sup> Such as the federal law against breaking ‘the seal or lock of any railroad car, vessel, aircraft’ (18 USC § 2117).

<sup>31</sup> Besek op cit note 2 at 441.

<sup>32</sup> For a more complete discussion of analogous state laws, see Besek op cit note 2 at 441-443.

if the United States legislature never discussed the necessity of a new access right, and such a right was not expressly introduced by the DMCA.<sup>33</sup> However, what the United States legislature did was to insert two separate provisions – to prohibit the act of circumventing access control technologies, and to prohibit the trafficking in devices that would enable a user to gain access to protected works.<sup>34</sup>

Section 1201(a)(1) of the Copyright Act now prohibits the circumvention of measures that prevent unauthorized *access* to a work protected by copyright. There is no similar prohibition on conduct relating to the circumvention of copy control technology. Also, section 1201(a)(1) prohibits the act of circumventing an access control even when *no infringement* follows.<sup>35</sup>

But why prohibit only conduct relating to the circumvention of access controls and not conduct relating to the circumvention of copy controls? Traditionally, unauthorized access to a copyright work was never regarded as copyright infringement. Where a protection measure was circumvented merely to gain access to a copyright work, such circumvention would not have led to liability for copyright infringement. So the United States legislature had to prohibit such unauthorized access expressly. However, when a protection measure is circumvented in order to perform any of the acts exclusively reserved for the author, the unauthorized performance of such an act would constitute infringement. Accordingly, as the circumvention of a copy control would in any event have amounted to an infringement it was not necessary to prohibit it expressly.<sup>36</sup>

Section 1201(a)(2) contains the technology related prohibition – it prohibits the making or distribution of a device used to circumvent a technological measure that prevents access to a work. This provision, then, targets those who facilitate the process of accessing a work.<sup>37</sup>

Although the Copyright Act does not expressly provide for an access right, it seems as if these two provisions indirectly recognize an access right. Section 1201(a)(1) and (2) protects measures that control access. While copyright law is concerned with the protection of rights,

---

<sup>33</sup> Koelman op cit note 15 at 276.

<sup>34</sup> Koelman op cit note 15 at 275; Van Coppenhagen op cit note 24 at 447.

<sup>35</sup> Jonathan Band 'The Digital Millennium Copyright Act: A Balanced Result' [1999] *European Intellectual Property Review* 92.

<sup>36</sup> Ficsor op cit note 11 at 551 C11.15.

<sup>37</sup> David Nimmer 'A Riff on Fair Use in the Digital Millennium Copyright Act' (2000) 148 *University of*

by providing protection for access control measures it seems as if the Act indirectly recognizes an access right.<sup>38</sup>

In *Lexmark International Inc v Static Control Components Inc*,<sup>39</sup> the court reasoned that the DMCA created a new exclusive right to control access to works protected by technological measures. The court expressly stated that an author's right to protect her work against unauthorized access was a right separate and distinct from her right to protection against violations of her exclusive rights such as reproduction and distribution. Here the court recognized that the DMCA created a new right for authors – the access right:<sup>40</sup>

'The DMCA is clear that the right to protect against unauthorized access is a right separate and distinct from the right to protect against violations of exclusive copyright rights such as reproduction and distribution.

'If the DMCA were only intended to protect copyrighted works from digital piracy, that goal was accomplished through section 1201(b); SCC's argument would render section 1201(a)(2) mere surplusage. Section 1201(a) creates, and section 1201(a)(2) protects, a right of "access", the violation of which is the "electronic equivalent [of] breaking into a castle.'

An author can now bring a civil action in court against any person who obtains access to her work without her authority.<sup>41</sup>

### 7.5.3 The European Union

The European Union protects access control within a broad framework of access to information services (the Conditional Access Directive<sup>42</sup>), and access to works protected by

---

*Pennsylvania Law Review* 673 at 687.

<sup>38</sup> Melissa A Kern 'Paradigm Shifts and Access Controls: An Economic Analysis of the Anticircumvention Provisions of the Digital Millennium Copyright Act' (2002) 35 *University of Michigan Journal of Law Reform* 891 at 893.

<sup>39</sup> Supra note 10.

<sup>40</sup> At 969.

<sup>41</sup> Koelman op cit note 15 at 275.

<sup>42</sup> Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, and consisting of, conditional access (the 'Conditional. Access Directive').

copyright, related rights, and databases (the Software,<sup>43</sup> the Database,<sup>44</sup> and the Copyright Directives<sup>45</sup>).

### 7.5.3.1 The Database Directive<sup>46</sup> and the Computer Programs Directive<sup>47</sup>

One could perhaps argue that an access right has been introduced into copyright law through the right to prohibit temporary reproductions, granted by the Computer Programs Directive<sup>48</sup> and the Database Directive.<sup>49</sup> Under these two Directives, any unlawful user who accesses a database or a computer program may be held liable for copyright infringement, as to access a digitized database or a computer program it must – at the current state of technology – temporarily be reproduced in the computer’s random access memory.<sup>50</sup>

Koelman<sup>51</sup> questions why an access right as such was not introduced independently of whether or not a technological measure prevents access. A similar question arises with regard to the Software and Database Directives: why was a right of access granted ‘in the disguise’ of the right of temporary reproduction?

Article 7(1)(c) of the Computer Programs Directive obliges Member States to provide appropriate remedies against any 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’ (emphasis added). So the Directive protects only those technological protection measures that *protect* computer programs. It does not distinguish expressly between access and copy control.

### 7.5.3.2 The Copyright Directive

---

<sup>43</sup> Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs. Official Journal L 122, 17/05/1991 P. 0042 – 0046 (the ‘Computer Programs Directive’).

<sup>44</sup> European Parliament and Council Directive 96/9/EC of March 11, 1996, on the Legal Protection of Databases, OJ EC L 77 (the ‘Database Directive’).

<sup>45</sup> Directive 2001/29/EC of the European Parliament and the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (the ‘Copyright Directive’).

<sup>46</sup> Op cit note 44.

<sup>47</sup> Op cit note 43.

<sup>48</sup> Ibid.

<sup>49</sup> The Database Directive op cit note 44.

<sup>50</sup> Koelman op cit note 15 at 275.

### 7.5.3.2.1 Article 2

Even though article 2 of the Directive grants an exclusive right to prohibit temporary reproduction, this right is limited by article 5.1 if the sole purpose of such reproduction is to enable ‘(a) a transmission in a network between third parties by an intermediary, or (b) a lawful use’. So the Directive does not exempt temporary reproductions for unlawful use. Currently, access to digital works entails temporary reproduction in the computer’s random access memory. Even if a work is not protected by access control, but access entails a temporary reproduction, any unlawful access would also amount to copyright infringement (unauthorized temporary reproduction constitutes copyright infringement). The distinction between this type of access and the one provided for under article 6 is, of course, that liability arises for copyright infringement in the event of unauthorized access, and not for circumventing access controls.

This is similar to the access right indirectly introduced through the right to prohibit temporary reproduction, granted in the Computer Programs Directive<sup>52</sup> and the Database Directive.<sup>53</sup>

### 7.5.3.2.2 Article 6

Article 6.1 of the Copyright Directive obliges Member States to ‘provide adequate legal protection against the circumvention of any effective technological measures’; article 6.2, in turn, 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 circumvention devices. In a nutshell, then, article 6.1 prohibits the act of circumvention, and article 6.2 the trafficking in circumvention devices.

These two articles are aimed at the protection of technological measures against circumvention. Article 6.3 then defines a ‘technological measure’:

‘Any technology, device or component that, in the normal course of its operation, is

---

<sup>51</sup> Idem at 276.

<sup>52</sup> The Computer Programs Directive op cit note 43.

designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorized by the right holder of any copyright or any right related to copyright as provided for by law or the *sui generis* rights provided for in . . . [the Database] Directive....’

Since access is not a ‘right related to copyright’ or the *sui generis* database right, it would at first blush seem as if only copy control (which protects an author’s traditional exclusive reproduction right) is protected. But article 6.1 does not protect all ‘technological measures’ but only ‘effective’ technological measures. In terms of article 6.3, a technological measure is deemed to be ‘effective’ where ‘[t]he use of a protected work or other subject-matter is controlled by right holders through 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’ (emphasis added). The ‘effective technological measures’ referred to in article 6.1, therefore, include both access and copy controls (‘protection process’). Once again, as is the position under the United States Copyright Act and the Conditional Access Directive, the Copyright Directive recognizes an access right by protecting access control technologies.

The Copyright Directive protects against unauthorized access to a work protected by copyright, whereas the Conditional Access Directive protects against unauthorized access to a protected service. Since some services consist of providing copyright works, accessing the service and such works will often be one and the same thing.<sup>54</sup> So the technological measures that prevent unauthorized access to a service will often also effectively protect the copyright content of the service.<sup>55</sup> Although the Conditional Access Directive aims to protect services rather than works, and although authors as such are not granted an action in court,<sup>56</sup> authors who deal directly with their customers will probably qualify as (information) service providers for purposes of the Conditional Access Directive. An example would be where an

---

<sup>53</sup> The Database Directive op cit note 44.

<sup>54</sup> Koelman op cit note 15 at 277; Thomas Vinje ‘Copyright Imperilled’ [1999] *European Intellectual Property Review* 192 at 205-206.

<sup>55</sup> Vinje op cit note 54 at 205 and 205-206 note 98.

<sup>56</sup> Commentary with Art 1(g) in the Explanatory Memorandum to the Conditional Access Directive: ‘(C)opyright and related rights do not fall within the field co-ordinated by the Directive: the interests protected by the proposed measures are the remuneration of service providers. Even though, from an economic point of view, rightholders will certainly benefit from such measures, this will be an indirect effect, and their interests remain distinct’ (cited by Koelman op cit note 15 at 277n42).

author requires a password for a user to gain access to a website from which her works are distributed on the Internet. The Conditional Access Directive also requires certain remedies to be available to service providers.<sup>57</sup>

The European Union thus created several types of access right: the right to control access to information services, the right to control access to copyright works, the right to control access to works protected by related rights and the right to control access to databases. This is far broader than the United States recognition of an access right to copyright works.

Acknowledging a right to control access to works is not as foreign to legal tradition as the recognition of a right to control access to information or information services. The EC chose to recognize both.<sup>58</sup>

#### **7.5.4 South Africa**

Although South Africa is a signatory of the WCT, it has yet to implement its provisions. Indeed, South Africa has no legislation aimed exclusively at the regulation of copyright in a digital environment. The Copyright Act<sup>59</sup> was drafted long before the digital era and is thus more suited to the analogue world.

Although South Africa has no legislation aimed at the protection of copyright in the digital environment, the Constitution of the Republic of South Africa, 1996,<sup>60</sup> and the Electronic Communications and Transactions Act<sup>61</sup> both contain provisions relevant to the present discussion. The Constitution does not expressly recognize a right to control access to information. But the Constitution does recognize a right to access to information, which has been fleshed out in the Promotion of Access to Information Act<sup>62</sup> and the South African Law Commission's proposed Data Protection and Privacy Act.<sup>63</sup> The ECT Act recognizes an access right in respect of data.

##### **7.5.5.1 The Constitution of the Republic of South Africa**

---

<sup>57</sup> Article 5 of the Conditional Access Directive.

<sup>58</sup> Koelman op cit note 15 at 277-278.

<sup>59</sup> Act 98 of 1978.

<sup>60</sup> Act 108 of 1996 (the 'Constitution').

<sup>61</sup> Act 25 of 2002 (the 'ECT Act').

<sup>62</sup> Act 2 of 2000.

The Constitution took effect on 4 February 1997. Chapter 2 of the Constitution contains the Bill of Rights. Only three of the rights entrenched in the Bill of Rights are relevant for present purposes – the right to property, the right to education, and the right of access to information. The right to property safeguards the rights of authors, whereas the latter two rights concern user privileges.

Section 25 safeguards ‘property’ and is specifically aimed at the protection of property against arbitrary deprivation:

‘No one may be deprived of property except in terms of law of general application, and no law may permit arbitrary deprivation of property.’

According to the Constitutional Court,<sup>64</sup> the concept ‘property’ includes intellectual property.<sup>65</sup> Even though this section recognizes the right of a person not to be deprived of his ‘property’, it does not recognize a right to control access to property.

Section 29 deals with the right to education, which includes basic and further education. But although the State has to ensure effective access to education, this provision stops short of extending the right to educational materials, such as textbooks subject to copyright. So this provision likewise does not confer on users a right to demand access to such works.

Section 32 creates a right of access to any information held by the State, or ‘that is held by another person and that is required for the exercise or protection of any rights’. Note that this right does not create a general right of access to information but is narrowly circumscribed. Only where the information required falls within the narrow ambit of this section, and is contained in a copyright work can a user seek to enforce this access right.

#### **7.5.5.2 The Electronic Communications and Transactions Act**

---

<sup>63</sup> Released in October 2005.

<sup>64</sup> See *Ex parte Chairperson of the Constitutional Assembly: In re Certification of the Constitution of the Republic of South Africa, 1996* 1996 (4) SA 744 (CC) in par [75].

<sup>65</sup> For comment on this ruling, see OH Dean ‘The Case for the Recognition of Intellectual Property in the Bill of

The ECT Act regulates electronic communications and transactions. The key concept ‘data’ is extensively defined as ‘electronic representations of information in any form’.<sup>66</sup> The definition of ‘data’ is broad and includes any type of digital information, such as digital copyright works.

Section 86(1), then, criminalizes the unlawful accessing of data: ‘[a]ny person who intentionally and unlawfully accesses or intercepts any data without authority or permission to do so, shall be guilty of an offence’. Section 86(3), in turn, states that ‘[a] person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence’. By criminalizing unlawful access as well as the trafficking in devices designed to bypass access control, the ECT effectively recognizes an access right.

Both provisions expressly refer to access. Section 85 defines ‘access’ as including ‘the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorized to access that data and still continues to access that data’.

Read together in this copyright context, these prohibitions cover both access not covered by a statutory copyright exception or limitation, and, in the absence of such exception or limitation, access not authorized by the author.

A teaser: the prohibitions in section 86 are directed at unauthorized and unlawful access, whilst the term ‘access’ ‘includes’ access by a person who, after becoming aware of the fact that she is not authorized to access the data, continues to do so. Does it follow, then, that these prohibitions also strike at access without any knowledge of the unauthorized nature of the access, and so impose strict criminal liability? Not only does this go far beyond the knowledge requirement of the WCT but it also flies in face of the general principles of criminal law.

---

Rights’ (1997) 60 *Tydskrif vir die Hedendaagse Romeins Hollandse Reg* 105.

<sup>66</sup> Section 1 of the ECT Act.

The term ‘strict criminal liability’ refers to criminal liability without proof of intention or negligence.<sup>67</sup> Strict criminal liability applies only to statutory offences. However, the theory of strict liability is frowned upon by many - not only because of the universal and fundamental nature of fault as a requirement of criminal liability in all civilised legal systems, but also because the normal principles of statutory interpretation would ordinarily require fault as an element of statutory offences.<sup>68</sup>

In *S v Coetzee & others*,<sup>69</sup> the Constitutional Court gave a strong indication that strict liability under South African criminal jurisprudence was unacceptable.<sup>70</sup> Snyman<sup>71</sup> argues that strict criminal liability can be contrary to the right to a fair trial,<sup>72</sup> as well as the right to freedom and security of the person.<sup>73</sup>

The answer to whether section 86 imposes strict liability, of course, lies in section 86(1) which expressly requires that the access must be intentional, which rules out any prospect of strict criminal liability. There is no such express knowledge requirement in section 86(3), and thus the question as to whether this subsection imposes strict criminal liability remains pertinent.

Finally, note that the ECT Act creates criminal liability only. It does not provide for any civil remedies.

## **7.6 Distinguishing Between Unauthorized Access and Circumvention**

The concept ‘unauthorized access’ is broader than ‘circumvention’. Unauthorized access does not require the existence of a technological protection measure, whereas the key element of circumvention is the existence of a technological protection measure that serves as a barrier between the user and the protected work. Before a user can access the protected work, she

---

<sup>67</sup> Jonathan Burchell *Principles of Criminal Law* (2005) at 545-546.

<sup>68</sup> *Ibid.*

<sup>69</sup> 1997 (3) SA 527 (CC).

<sup>70</sup> Burchell *op cit* note 67 at 550.

<sup>71</sup> CR Snyman *Strafreg* (2006) at 245.

<sup>72</sup> Section 35(3) of the Constitution.

<sup>73</sup> Section 12(1) of the Constitution.

must bypass the technological protection measure.<sup>74</sup> ‘Access’ statutes, such as the United States Stored Wire and Electronic Communications Act<sup>75</sup>, and the Computer Fraud and Abuse Act,<sup>76</sup> are concerned with the user’s unauthorized contact with the protected material. Anti-circumvention legislation, by contrast, focuses on actions with respect to the technological protection measures that protect the material.<sup>77</sup>

This distinction was made very clear in *IMS Inquiry Management Systems Ltd v Berkshire Information Systems*.<sup>78</sup> In this case the court held that Berkshire’s use of an IMS customer’s password to access IMS’s website did not amount to ‘circumvention’ under section 1201 of the Copyright Act. However, IMS did have a claim under the Computer Fraud and Abuse Act, which prohibits intentional and unauthorized access to a protected computer but does not require that the access be obtained through the circumvention of technological protection measures.<sup>79</sup>

## **7.7 Users and the Access Right**

### **7.7.1 Consequences of the Access Right**

The new access right of authors would probably have the greatest impact on users’ ability to make use of copyright works. I shall now discuss a few consequences of the recognition of this new right.

#### **7.7.1.1 Access Control and the Prevention of Use**

The most obvious result of the recognition of an access right access is that authors will have unlimited control over their works – the person who controls access to a work also controls its use. Although copyright law traditionally prohibits several instances of unauthorized use, it does not prohibit *all* use. So copyright law does not confer an exclusive right to control *all*

---

<sup>74</sup> Besek op cit note 2 at 444.

<sup>75</sup> 18 USC.

<sup>76</sup> Ibid.

<sup>77</sup> Besek op cit note 2 at 445.

<sup>78</sup> 307 F Supp 2d 521 (SDNY 2004).

<sup>79</sup> Besek op cit note 2 at 445.

use or consumption of a work.<sup>80</sup> Were authors to have the exclusive right to control access to their works, they will be capable of controlling *all* use of their works.<sup>81</sup>

The first implication of unlimited control is, of course, that the legitimate use allowed for by the exceptions and limitations in copyright laws may be eroded. The right to control access to a work, and hence the consumption of such work, is separate and distinct from an author's traditional exclusive rights. It is uncertain whether the traditional copyright limitations and exceptions apply to the new exclusive access right. As the access right is now recognized as an exclusive right, it should also be subject to limitations and exceptions.<sup>82</sup> If it were not expressly limited to allow legitimate use, the access right may effectively stifle legitimate and fair uses – fair users would need authorization to access a work (or an exception that allows for such access) before they would be entitled to make fair use of the protected work.

Unlimited access control also implies that authors can control the mere browsing of their works. Books serve as a good example: in the analogue world, potential buyers were entitled to page through a book, read passages from it, or glance at the table of contents to assist them in their decision whether or not to buy the book. In the digital environment, potential buyers usually have to rely on the title of a work in order to decide whether they want to buy it. However, even though authors may now be entitled to prevent the browsing of their works, it does not mean that they necessarily do so in practice. The famous website *Amazon.com* now allows potential buyers to browse the books for sale on there. Unfortunately, this is not yet the case with e-books.

The pessimists believe that authors, by controlling access, may end up completely preventing use.<sup>83</sup> But authors earn revenue from the use of their works, and in most cases they will be able to sell their works only if the public is familiar with them. Protected works need a certain amount of public exposure to make them marketable. I believe, therefore, that it is doubtful that authors would indeed want to prevent all use of their works. The types of use that would obviously be targeted by authors are infringing use. It goes without saying that authors want to prevent infringing use (and, by statute, they are entitled to do so).

---

<sup>80</sup> Jessica Litman *Digital Copyright* (2001) at 13 and 28; Koelman op cit note 1.

<sup>81</sup> Litman op cit note 80 at 80; Koelman op cit note 1.

<sup>82</sup> Ginsberg op cit note 1 at 148.

<sup>83</sup> Ginsberg op cit note 1 at 143.

### 7.7.1.2 Access Control and Payment-per-use

A second consequence of recognizing access control as an exclusive right, is that copyright legislation now allows authors legally to monitor each access to (and subsequent use of) their works. Such monitoring is already possible by means of metering technologies.<sup>84</sup> It is interesting to note that the legislation protecting technological protection measures does not explicitly protect these metering technologies, since, strictly speaking, they do not control access or prevent infringement. It seems, then, as if metering technologies that facilitate the enforcement of the protection of technological protection measures, themselves are not protected.<sup>85</sup>

The fact that authors can now monitor the initial and every subsequent access to their works has cost implications. An author can now charge not only for the acquisition of a copy of her work but also for each subsequent access.<sup>86</sup> Unlike the position in the analogue environment, users can now be charged for each subsequent access to a work. But this enables authors to use new distribution models, such as the ‘pay per use’ model. These models give users the opportunity to read, view, or experience the works, without imposing the costs of an unlimited access option (this was the only available option in the analogue world – a user had to obtain the work in order to access it). *iTunes*, *Movielink*, *CinemaNow*, and *Soapcity* are some examples of ‘pay per use’ models.<sup>87</sup> However, the ability to charge for subsequent use could lead to unfair results if authors keep the cost of obtaining initial access the same than it was for obtaining the work in the analogue world, where the same fee covered obtaining initial access and unlimited subsequent access to the work. So authors should lower the cost of initial access, as initial access no longer includes subsequent unlimited free access. The revenue lost by lowering the cost of initial access will, in any event, be made good by the additional revenue authors will receive for each subsequent access.

### 7.7.1.3 Access Control and User Privacy

---

<sup>84</sup> Koelman op cit note 15 at 277.

<sup>85</sup> Idem. At 277 note 37.

<sup>86</sup> Ginsberg op cit note 1 at 147.

<sup>87</sup> Besek op cit note 2 at 474.

The ability of authors to monitor access to (and hence also the use of) their works makes it easier to control copying by authorized and known users. It can also help to prevent copyright infringement, or to detect copyright infringement after it occurred.<sup>88</sup> However, such ability may also have serious privacy implications for users. In the digital world, private individuals access works, and so unauthorized access can be detected only by policing private behaviour. Enforcing a prohibition on the circumvention of access control involves entering into a user's private sphere. This type of policing has been made possible by metering technology,<sup>89</sup> which reveals not only the type of information accessed but also the identity of the person who accessed it. The question arises – it is desirable, in an open and democratic society, to allow the use of metering technology of this kind, even if it is not use by official bodies but by private entities?<sup>90</sup> I think not.

#### **7.7.1.4 Access Control and the Lawful Possession of a Physical Embodiment**

The recognition of the fact that access to a work can be distinguished from access to a physical copy of such work can also have some implications for someone in possession of a physical copy of a work. As I have indicated, physical possession of a copy of a work no longer guarantees access to the embedded work. For a person unlawfully in possession of a copy of a work, this presents no problem – our sense of justice does not allow such a possessor access to the embedded copyright work. But what is the position of a lawful possessor? Should a lawful possessor be allowed unlimited access to the work, simply by virtue of the fact that she is lawfully in possession of a physical copy of a work?

Two contrasting arguments can be made. On the one hand, one can argue that the lawful possessor must be allowed unlimited access to the work, and that, accordingly, she may circumvent any access controls that prevent her from having access to the work. On the other hand, one can argue that as access to a copy of a work and access to a work are completely separate acts, access to a copy does not necessarily imply authorization to access the embedded work.

---

<sup>88</sup> NA Smith 'United States of America' in M Dellebeke (ed) *Copyright in Cyberspace*, ALAI Study Days in Amsterdam, 4-8 June 1996 (1997) at 418, cited by Koelman op cit note 15 at 276.

<sup>89</sup> Koelman op cit note 15 at p 276.

<sup>90</sup> Koelman op cit note 15 at 277.

Case law on section 1201(a)(2) of the United States Copyright Act (such as *CSC Holdings Inc v Greenleaf Electronics Inc*,<sup>91</sup> *Sony Computer Entertainment America Inc v Gamemasters*,<sup>92</sup> and *Realnetworks Inc v Streambox Inc*<sup>93</sup>) dealt with technologies that allow a user to view or use content that she has not lawfully acquired. Unfortunately, then, these cases offer no guidance for interpreting section 1201(a)(2) with respect to content lawfully acquired by a user.

To Van Den Elzen<sup>94</sup> it seems as if a circumvention device will not be regarded as such where the user already had lawful access to the work. He draws an analogy between the circumvention of technological measures and breaking into a locked room in order to obtain a copy of a book. He then states that this analogy does not apply to DeCSS (a computer program capable of decrypting content encrypted by the Content Scrambling System (CSS)):

‘In order to use DeCSS to decrypt a DVD one must first have the DVD. Once a person purchases a DVD that person arguably has obtained authorized access to the motion picture. To say that a person cannot use DeCSS to view the DVD is like selling a book that comes with a locking mechanism on the binding preventing the purchaser from reading the book and saying that the only acceptable means of unlocking the book is a key specifically licensed by the publisher.’

Put differently, Van Den Elzen argues that mere ownership of a Digital Versatile Disc (DVD) is enough for authorized access. There is even a stronger argument that ownership of both the DVD and a licensed DVD drive provides the user with authorized access.

He also quotes a passage from the House Judiciary Report on the DMCA that indicates that section 1201(a) was not intended to apply to situations like DVD owners using DeCSS:<sup>95</sup>

‘Paragraph (a)(1) does not apply to the subsequent actions of a person once he or she has obtained authorized access to a copy of a work protected under Title 17, even if

---

<sup>91</sup> 2000 U.S. Dist. LEXIS 7675 (N.D. Ill. 2000).

<sup>92</sup> F Supp 2d 976 (ND Cal 1999) at 987-88.

<sup>93</sup> No C99-207OP, 2000 US Dist LEXIS 1889 (WD Wash).

<sup>94</sup> Ryan L Van Den Elzen ‘Decrypting the DMCA: Fair Use as a Defense to the Distribution of DeCSS’ (2002) 77 *The Notre Dame Law Review* 673 at 680-681.

<sup>95</sup> *Ibid.*

such actions involve circumvention of additional forms of technological protection measures. In a fact situation where the access is authorized, the traditional defenses to copyright infringement, including fair use, would be fully applicable. So, an individual would not be able to circumvent in order to gain unauthorized access to a work, but would be able to do so in order to make fair use of a work which he or she has acquired lawfully.<sup>96</sup>

So it seems to follow that a person who purchases a DVD lawfully acquires a copy of the film recorded on the disc and so has authorized access to the film. As she has lawfully acquired the film, she may then legally circumvent any additional type of technological protection.<sup>97</sup>

Van Den Elzen<sup>98</sup> states that the legislative history of the access control provisions introduced by the DMCA imply that they were intended to prevent the interception of online transmissions of copyright works, and not to prevent access to a work that a consumer has purchased. He equates access to a copy of a work and access to a work. Whilst it is true that the access control provisions should not prevent access to an underlying work where a user purchased the underlying work, the provisions should prevent access where a user merely bought a copy of a work and not the underlying work itself. For example, where the user bought only one of several works contained in the same physical medium, she should be refused access to *all* the embedded works since he or she obtained only *one* legally, even if she legitimately obtained the physical copy of the works. In any event, this seems to be a highly hypothetical situation – whether authors will actually sell their works in this manner remains to be seen. So the question is not whether the user lawfully obtained a copy of the work (the physical embodiment), but rather whether the user obtained the embedded work lawfully.

A more practical problem arises where a user lawfully obtains a work in a certain country, and the work is licensed for distribution and use only in that country. Typically such a work is encrypted, and the playback devices sold in that country verify that the work is an

---

<sup>96</sup> HR Rep No 105-551, pt1, at 18. The Senate Judiciary Committee stated: ‘This paragraph does not apply to subsequent actions of a person once he or she has obtained authorized access to a copy of a work protected under Title 17, even if such actions involve circumvention of other types of technological protection measures’ (S Rep No 105-190, at 28 (1998)).

<sup>97</sup> Van Den Elzen op cit note 94 at 682.

<sup>98</sup> Idem at 683.

authorized legitimate product licensed for distribution in that geographical territory before the user can gain access to the work. The user can access the work on a playback device sold in another geographical area only if the technological protection measure (encryption) is circumvented. In two cases, *Universal City Studios, Inc v Corley*<sup>99</sup> and *321 Studios v Metro Goldwyn Mayer Studios Inc et al*,<sup>100</sup> it was held that the purchase of a DVD does not give the purchaser the author's consent to decrypt CSS (the technological protection measure). By lawfully obtaining a DVD, a user has the authority to view the encrypted content but not the authority to decrypt the content. In *Sony Computer Entertainment America Inc v Gamemasters*,<sup>101</sup> the court distinguished between a security system function preventing the use of pirated copies of video games in a video game console and another function through which the use of legitimate copies of video games may be limited to those sold in the same territory in which the console is sold. The court held that even the distribution of a 'game enhancer' device whose primary function was to circumvent a code limiting the use of a video game to a limited territory was prohibited by section 1201(a)(2) of the Copyright Act. This means that even a person in possession of a lawful copy of a work may not circumvent protection measures to use the work herself. In the present case, the technological measure that prevented access to the software embedded in Sony's *Playstation* console was seen as access control, and the device that circumvented this measure was found to be a circumvention device, even though it did not facilitate piracy.<sup>102</sup>

It seems as if the courts in these two cases failed to distinguish between a work and a copy of a work. Where a user buys a legitimate copy of a work such as a DVD, the user obtains the embedded work, too, and not only the physical embodiment of the work. It seems to me as if such a user should indeed be allowed to circumvent the protection measure – if not in terms of copyright law, definitely in terms of the law of contract. The user bought the embedded work in terms of the law of contract, and so should be allowed to use and enjoy it. A person with both the legitimate work (the DVD) and a licensed DVD drive surely has authorized access to the work.<sup>103</sup>

---

<sup>99</sup> 272 F 3d 429 (2d Cir 2001) at 444.

<sup>100</sup> 307 F Supp 2d 1085 (ND Cal 2004) at 1096.

<sup>101</sup> 87 F Supp 2d 976 (ND Cal 1999) at 981, 987 and 990.

<sup>102</sup> At 987.

<sup>103</sup> Van Den Elzen op cit note 94 at 683.

Also, the courts failed to consider the first sale doctrine.<sup>104</sup> This doctrine, the United States version of the doctrine of exhaustion, is to the effect that that the owner of a lawfully made copy of a work is entitled to ‘sell or otherwise dispose of the possession’ of that copy. The doctrine is founded on the right to alienate physical property and applies to physical copies, in digital or analogue form. According to Besek,<sup>105</sup> this means that there is a privilege to give away or sell a DVD containing an authorized copy of a film, but there is no first sale privilege electronically to retransmit a copy of a film downloaded via *Movielink*.

I agree with Besek’s argument. The first sale doctrine relates to physical copies. So a person in possession of a physical copy of a work is indeed entitled to sell such copy. But this doctrine does not apply to digital works sold or transmitted electronically only – it applies only to digital works embedded in physical copies. If it were to apply to digital works, legislation should expressly provide for that.

In the United States, section 1621 of the Copyright Act,<sup>106</sup> currently pending, attempts to create a digital first sale doctrine that would allow transmission of a digital copyright work, as long as the original work is deleted.<sup>107</sup> The Copyright Office rejected the notion that requiring copies of works to play on a particular platform interferes with user privileges under the first sale doctrine. Regional limitations accordingly do not interfere with user privileges. Also, the Office rejected requests for an exemption to enable platform shifting.<sup>108</sup> This is clearly wrong. In these instances the user lawfully acquires the physical copy as well as the embedded copyright work. The user contracted for the embedded work and should be entitled to use and enjoy the merx (the embedded copyright work) even if this would entail the circumvention of a regional limitation control.

Recently, in *Stevens v Kabushiki Kaisha Computer Entertainment*,<sup>109</sup> the High Court in Australia held that the act of lawfully acquiring a program in one country and then playing it in another is not copyright infringement. So Sony’s goal of dividing the world through

---

<sup>104</sup> 17 USC § 109.

<sup>105</sup> Besek op cit note 2 at 473.

<sup>106</sup> S 1621, 108th Cong (1st Sess 2003) (introduced by Senator Brownback on 16 Sept 2003).

<sup>107</sup> Besek op cit note 2 at 505.

<sup>108</sup> *Idem* at 473.

<sup>109</sup> [2005] HCA 58 (6 October 2005) at par 47, 175 discussed in Andrew Manning & John Selby ‘A Fine Line Between Legal Access and Circumvention: The Australian High Court Provides a Pyrrhic Victory for the Sale of Mod-chips’ [2005] *Computer und Recht International* 161 at 162.

copyright law into three mutually exclusive economic regions was denied judicial acceptance in Australia.<sup>110</sup> Unfortunately, the implementation of the US Free Trade Agreement Implementation Act of 2004<sup>111</sup> brings the Australian Copyright Act<sup>112</sup> in line with the higher level of protection in the United States Copyright Act, which would nullify this decision.

### 7.7.2 The Emergence of a Corresponding User ‘Right’ to Demand Access?

Did the access right create a balancing right for users to demand access? Many users believe that they have a right to use a copyright work in accordance with a copyright exception or limitation. But this is not true – a user does not have the right to demand the use of a work. It is the author alone who holds rights to her works; a user merely enjoys those privileges that copyright law provides by means of limitations on and exceptions to the author’s exclusive rights.<sup>113</sup>

Guibault<sup>114</sup> discusses the legal nature of copyright limitations and exceptions. She investigates whether user privileges create enforceable subjective rights (similar to the author’s exclusive rights). She analyzes the nature of a subjective right in Europe and indicates the following four characteristics of a subjective right: (a) a close relationship – or interest – between the subject and the object, which relationship is recognized by the positive law; (b) the subject’s exclusive power of control over the object, to which a number of prerogatives are attached; (c) the existence of a correlating duty on the public to respect the subjective right; and (d) the recognition of a right of action to guarantee the enforcement of the subjective right.

The author’s exclusive rights exhibit all four characteristics.

However, when she looks for these characteristics in copyright limitations, Guibault concludes that, contrary to the general characteristics of a subjective right, the authorization

---

<sup>110</sup> Manning & Selby op cit note 109 at 163.

<sup>111</sup> Act 120 of 2004, Schedule 9 accessible at <<http://scaleplus.law.gov.au/html/comact/browse/TOCUS.htm>> (visited on 29 January 2007)

<sup>112</sup> 1968.

<sup>113</sup> Christopher Geiger ‘Right to Copy v. Three-Step Test The Future of the Private Copy Exception in the Digital Environment’ [2005] *Computer und Recht International* 7 at 8.

<sup>114</sup> Lucie MCR Guibault *Copyright Limitations and Contracts: An Analysis of the Contractual Overridability of Limitations on Copyright* (doctoral thesis Amsterdam, 2002) at 90-110.

to make legitimate use of a copyright work is neither exclusive to one user nor to one work. Only a few of the prerogatives that normally derive from the recognition of a subjective right are present in the context of the authorization to make legitimate use of a protected work. As users have no power of control over the protected work, there is no corresponding obligation to respect the user's 'interest' in making legitimate use.<sup>115</sup> And, of course, a user has no right of action to guarantee the enforcement of her interest. From this it is clear that the user's interest cannot be elevated to a subjective right. Even though the notion of a subjective right is unknown to the American common law, Guibault<sup>116</sup> reaches a similar conclusion about the nature of copyright limitations and exceptions in the United States.

It also seems appears that the courts do not hold the view that users have a right to demand making legitimate or fair use of a protected work. In *United States v Elcom Ltd*,<sup>117</sup> the court stated that 'there is as yet *no generally recognized right* to make a copy of a protected work, regardless of its format, for personal non commercial use'.<sup>118</sup> It also rejected the argument that users have a right to 'the most technically convenient way to engage in fair use'.<sup>119</sup> Fair use cannot be used as a basis for instituting action – it is merely a defence against an action for copyright infringement.<sup>120</sup> This position has been confirmed in European cases dealing with the private copy exception. Both the Paris District Court<sup>121</sup> and the Brussels District Court<sup>122</sup> held that the private copy exception grants no rights whatsoever to the user. According to the Paris court, the 'legislature did not intend to provide simply anyone with the right to make a private copy of every work',<sup>123</sup> whilst, according to the Brussels court,<sup>124</sup>

'the private copy rule is not a right but an exception. . . . The exception only means

---

<sup>115</sup> *Idem* at 93.

<sup>116</sup> *Idem* at 94-95.

<sup>117</sup> 203 F Supp 2d 1111 (ND Cal 2002)

<sup>118</sup> At 1135 (emphasis added).

<sup>119</sup> At 1131.

<sup>120</sup> Sections 24 and 25 of the South African Copyright Act deal with the institution of actions. Section 24 recognizes the right of a copyright owner and section 25 the right of a licensee to institute an action for infringement. The Act does not recognize any user right to institute an action to demand use in terms of an exception.

<sup>121</sup> Decision of the Paris District Court, 3rd Chamber, 2nd Section, April 30, 2004, RIDA October 2004 (202), 323; Com. Comm. Électr. July-August 2004, 24, comment by C. Caron; JCP 2004, E, 1101, comment by T. Maillard; JCP 2004, G, II, 10135, comment by C. Geiger; Légipresse September 2004, 150, comment by M. Vivant/G. Vercken, cited by Geiger op cit note 113 at 7-8.

<sup>122</sup> Decision of the Brussels District Court, May 25, 2004, Auteurs & Médias 2004, 338, comment by S. Dusollier, cited by Geiger op cit note 113 at 7-8.

<sup>123</sup> Translated by Geiger op cit note 113 at 8 note 13.

<sup>124</sup> Translated by Geiger op cit note 113 at 8n13.

that it is not necessary to obtain the authorization from the copyright owner to make a copy of the work. . . . In this sense, it is nothing more than a legally granted immunity against prosecution.’

But no-one denies that users have an interest in making legitimate or fair use of a protected work. If this ‘interest’ cannot qualify as a subjective right, what type of ‘interest’ do users have? In European legal theory, the positive law ensures the protection of ‘legitimate interests’ of private individuals. By excluding these interests from the scope of copyright protection, the positive law allows users to exercise these legitimate interests without infringing the author’s copyright. The fact that the positive law excludes certain acts from the control of authors benefits all users of the protected work. As a result, the users obtain an objective right to perform the acts specified in the copyright laws. So the general protection of these interests gives rise to an ‘objective right’.<sup>125</sup> The practical equivalent of the European notion of an objective right in American common law is a privilege.<sup>126</sup>

Exceptions (or user privileges) merely limit the author’s exclusive rights. Exceptions do not found an action against the author – they are only defences against an action for copyright infringement.<sup>127</sup> Exceptions do not create any user rights, either.<sup>128</sup> So it seems logical that users do not have a right to demand access. A user who wants access to a protected work would only be able to do so without an access key if there is a specific exception allowing her such access.

The circumvention of access controls constitutes an unlawful act separate of copyright infringement.<sup>129</sup> Liability arises not for ‘copyright infringement’ but for circumvention of a

---

<sup>125</sup> Guibault op cit note 114 at 95-97.

<sup>126</sup> Idem at 97-99.

<sup>127</sup> For example, sections 24 and 25 of the Copyright Act deal with the institution of actions. These sections recognize only the right of an author or a licensee to institute an action for infringement. They do not recognize any user right to institute an action to demand use in terms of an exception.

<sup>128</sup> This has already been confirmed in American jurisprudence. In *Universal City Studios Inc v Corley* supra note 99 at 459, the court expressed doubt as to whether fair use was actually compelled by the First Amendment. It stated that there was in any event no constitutional requirement that fair use be made in the format of the original or in the user’s preferred format (see at 458). In *United States v Elcom Ltd* supra note 117, the court stated that ‘there is as yet no generally recognized right to make a copy of a protected work, regardless of its format, for personal noncommercial use’ (at 1135, emphasis added). It also rejected the argument that users have a right to ‘the most technically convenient way to engage in fair use’ (see at 1131).

<sup>129</sup> See Pete Singer ‘Mounting a Fair Use Defense to the Anti-Circumvention Provisions of the Digital Millennium Copyright Act’ (2002) 28 *University of Dayton Law Review* 111 at 128.

technological protection measure.<sup>130</sup> The unlawfulness of a violation of the circumvention prohibition is independent of whether such circumvention results in copyright infringement.<sup>131</sup> As circumvention is a violation distinct from copyright infringement, the exceptions that serve as defences against actions for copyright infringement are not be available against actions for the circumvention of technological protection measures.<sup>132</sup> So the access right is not subject to the same exceptions and limitations as the other exclusive rights of an author. Instead, it is subject to a different set of exceptions. In the pieces of implementing legislation I discuss in my thesis, these exceptions are narrow and specific.<sup>133</sup> There is also no general exception allowing users to make fair use of a work.

Even if a user were fortunate enough to find among these narrow exceptions one that would allow her to circumvent access control, she would not necessarily have the means to do so, as circumvention devices are also prohibited. So users have no technological tools at their disposal with which to perform the circumvention necessary to exercise their user privileges.<sup>134</sup> Only those who can design and make their own circumvention devices would be able to circumvent access control where any of the exceptions apply.<sup>135</sup>

The recognition of an access right, and the failure to limit this right sufficiently by exceptions, has an enormous impact on users' ability to use copyright works.

## 7.8 Conclusion

The international trend is towards the recognition of an access right as one of an author's exclusive rights to her digital works.<sup>136</sup> This is done indirectly by protecting the technological measures that control access. Griffiths and others<sup>137</sup> go so far as to state that 'the nature of the exclusive right known as copyright has evolved towards a right to control access as we move

---

<sup>130</sup> See Glynn S Lunney Jr 'The Death of Copyright: Digital Technology, Private Copying and the Digital Millennium Copyright Act' (2001) 87 *Virginia Law Review* 813 at 839.

<sup>131</sup> Jeanneret op cit note 1 at 168-169.

<sup>132</sup> Besek op cit note 2 at 394.

<sup>133</sup> See, for example, 17 USC § 1201(d)-(g).

<sup>134</sup> See Band & Isshiki op cit note 26 at 220; Jeanneret op cit note 1 at 167; Vinje op cit note 54 at 202. Compare Ginsberg op cit note 1 at 152-153, who argues that if a device is manufactured for a fair use, and used for fair use purposes, there would be no violation of section 1201(b).

<sup>135</sup> See Besek op cit note 2 at 394.

<sup>136</sup> Koelman op cit note 15 at 276.

<sup>137</sup> Griffiths & Suthersanen op cit note 16 in para 12.33 at 303.

into the digital age'. One can ask why the right to control access was not granted expressly and independently of whether or not a technological measure controls such access. According to Koelman,<sup>138</sup> perhaps one of the main reasons for not directly and expressly creating an access right is that to grant an action against non-commercial individual access to, or consumption of a work, would seem to constitute a revolution in copyright law – copyright law traditionally covers acts related to commercial exploitation performed by potential competitors and not the individual acts carried out by individual end users.

But was it really necessary to recognize an access right? As existing copyright law provides remedies against copyright infringement, why, Lipton<sup>139</sup> asks, should offenders be denied access in the first place? Historically, copyright in printed material was always considered to be effective without copyright statutes preventing illegal access to locked offices, libraries, book stores, and filing cabinets. Why should the position be any different with digitally stored material? In the past, the law of trespass regulated unauthorized access to works stored physically in shops and in private possession. By the same token, should not the law of trespass, rather than copyright law, be revised to prevent or control similar access in the digital realm?<sup>140</sup> According to Lipton,<sup>141</sup> one may argue that the real problem is rather that the civil and criminal sanctions for trespass have not kept pace with the digital reality. Despite the fact that legislators in most jurisdictions try to deal with trespass in the digital environment,<sup>142</sup> such legislation was not successful for lack of effective enforcement, mainly because of jurisdictional and evidentiary concerns.<sup>143</sup> Given these problems, there is no reason to think that copyright laws attempting to achieve the same goal will be any more effective in terms of enforcement. Whether in terms of copyright law or the law of trespass, the question remains as to whether such legal protection can ever be truly effective – once again because of the problems of jurisdiction and obtaining evidence.<sup>144</sup>

To conclude: even where users are small enough to enter through the door of legitimate uses,

---

<sup>138</sup> Koelman op cit note 15 at 276.

<sup>139</sup> Jacqueline Lipton 'Copyright in the Digital Age: A Comparative Survey' (2001) 27 *Rutgers Computer & Technology Law Journal* 333 at 363.

<sup>140</sup> *Idem* at 363-364.

<sup>141</sup> *Idem* at note 91.

<sup>142</sup> See, for example, the Computer Misuse Act 1990 (England) and the Uniform Trade Secrets Act (United States of America).

<sup>143</sup> Lipton op cit note 139 at 364.

<sup>144</sup> *Ibid.*

this still does not mean that they will be able to access the garden of protected works. They face the same dilemma as Alice - they do not have the key to unlock the door, as it is the hands of the author.

## CHAPTER 8: CONCLUSION AND RECOMMENDATIONS

>AWould you please tell me, please, which way am I ought to go from here?@

>AThat depends a good deal on where you want to get to,@ said the Cat.=

Lewis Carrol

*Alice=s Adventures in Wonderland*

### 1 Introduction

In my thesis I looked at digitization and its effect on copyright law, and some of the means employed to secure digitized works that are protected by copyright. I concentrated on the technological protection measures used by authors to protect their works, the framework provisions of article 11 of the WIPO Copyright Treaty (WCT), and the legislation in the United States of America and the European Union to enable these countries to ratify the WCT. It has been a thread running through my thesis that many of these legislative provisions, while mindful of author's= interests, at the same pose a considerable threat to users of copyright works, especially to their ability to make lawful use of copyright works without needing to obtain authors= permission. Whether this threat is real, only time will tell.

In this chapter, I first highlight how this threat has been met in the United States of America and the European Union. I shall then make some recommendations about how article 11 should be implemented in South Africa.

### 2 Recommendations for Implementing Legislation Generally

In the course of my discussion of article 11 of the WCT, and the legal position in the United States of America and the European Union, I have noted how the copyright balance has become increasingly precarious B the demonstrated and undeniable threat to authors= interests in the digital era posed by the circumvention of technological protection measures has been met by sweeping protective legal measures seemingly balanced by rather narrow exceptions and limitations in favour of users. To inform my recommendations for legislative reform in South Africa, I shall first revisit briefly the threats to the copyright balance, how

they have been addressed, and how they have been avoided, in the United States and Europe.

## **2.1 Prohibit the Act of Circumvention, not Circumvention Devices**

Traditionally, copyright law deals with the exclusive right of an author to perform certain acts. Copyright law prohibits unauthorized acts, but not the devices with which such acts are (or can be) performed. In line with this tradition, article 11 of the WCT requires only the prohibition of the act of circumventing technological protection measures. However, as I have shown, in implementing the provisions of article 11 many legal systems opt also to prohibit the devices used for circumvention. This prohibition of circumvention devices can easily yield technological monopolies.

Accordingly, my first general suggestion for legislative intervention is that the prohibition should strike only at the act of circumvention but should not concern itself with the devices used to perform such circumvention. Not only would this be in line with traditional copyright law, but it obviates the problem of legitimate users being unable to use the circumvention devices they require to exercise their privileges under a copyright exception.

An added advantage of striking exclusively at the act of circumvention is that such a provision is far easier to reconcile with copyright limitations: a judge simply determines whether the act of circumvention served to infringe copyright.<sup>1</sup>

The main objection to this modest approach is that permitting the manufacture and distribution of circumvention devices for some non-infringing purposes effectively renders the anti-circumvention provision meaningless.<sup>2</sup> However, to design a norm that effectively rules out the availability of devices or services that enable the circumvention of technological protection measures and that respects user privileges under the copyright limitations and exceptions is not easy.<sup>3</sup>

---

<sup>1</sup> Kamiel J Koelman 'A Hard Nut to Crack: The Protection of Technological Measures' [2000] *European Intellectual Property Review* 272 at 279.

<sup>2</sup> June M Besek >Anti-Circumvention Laws and Copyright: A Report from the Kernochan Center for Law, Media and the Arts= (2004) 27 *Columbia Journal of Law & the Arts* 385 at 394.

<sup>3</sup> Koelman op cit note 1 at 279.

## 2.2 Create a General >Other Legitimate Purposes= Exception

Ever since anti-circumvention legislation was first proposed in the United States of America,<sup>4</sup> concerns have been raised that the protection of technological protection measures could jeopardize users' ability to make legitimate use of copyright works. This concern flows, of course, from the fact that the circumvention of technological protection measures is treated as an unlawful act distinct from copyright infringement. So the prohibition of the circumvention of technological measures is not subject to the same limitations and exceptions as copyright infringement. As I have shown, legislation implementing article 11 of the WCT invariably contains a separate list of exceptions created specifically for the circumvention prohibition. These exceptions are typically narrow, which can lead to the conclusion that any circumvention not expressly excepted is prohibited. The over-specification of special exemptions makes it difficult to articulate a general user privilege supporting the circumvention of technological protection measures.<sup>5</sup>

According to Samuelson,<sup>6</sup> there are many other legitimate reasons for circumventing that are not, strictly speaking, covered by the exceptions. To cite but one of her examples:<sup>7</sup>

>Suppose, for example, that a copyright owner had reason to believe that an encrypted work contained an infringing version of one of its works. The only way to find out whether the copyright owner's suspicion is valid may be to circumvent the technical protection system to get access to the encrypted material. Even if its suspicions proved correct, the copyright owner would have violated section 1201(a)(1)(A) in the course of discovering this. There is no exception in section 1201 to protect this kind of decryption activity.=

---

<sup>4</sup> In Chapter II of the Information Infrastructure Task Force *Intellectual Property and the National Information Infrastructure: A Preliminary Draft of the Report of the Working Group on Intellectual Property Rights: The Green Paper* (July 1994).

<sup>5</sup> Jane C Ginsberg >Copyright Legislation for the ADigital Millennium@= (1999) 23 *Columbia - VLA Journal of Law and the Arts* 137 at 151.

<sup>6</sup> Pamela Samuelson >Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised= (1999) 14 *Berkeley Technology Law Journal* 519 at 538, 543-546.

The creation of a general >other legitimate purpose= exception is thus suggested. An exception that allows circumvention for legitimate purposes implies that non-infringing uses would be excepted as they are legitimate.<sup>8</sup>

The main challenge of suggestion is to apply it in practice. It appears impossible to reconcile an effective protection of technological protection measures with exceptions, whether they be a narrow list, or a general >other legitimate use= exception. The application of many exceptions depends upon special circumstances, and technology cannot recognize whether an exception applies in a certain set of circumstances. So a technological protection measure may well block infringing *and* legitimate ones.<sup>9</sup> For this reason proponents of stronger copyright protection typically fear that permitting the manufacture and distribution of circumvention devices for some non-infringing purposes will effectively make the anti-circumvention provision legislation meaningless.<sup>10</sup>

Another alternative is to allow the technological protection of any use, but to permit at the same time the circumvention of such a measure, if the circumvention is necessary to perform a non-infringing act. The problem with this alternative is that most users do not have the technical abilities to circumvent technological protection measures, and are dependent on circumvention devices supplied by third parties. If such circumvention devices are not available, the copyright limitations will lose their meaning. But, because these devices cannot distinguish between infringing and non infringing uses, if it is available, anybody can obtain them and use them for infringing activities.<sup>11</sup>

### **2.3 Fair use by design**

---

<sup>7</sup> Idem at 543.

<sup>8</sup> Besek op cit note 2 at 390 and 476-485; Samuelson op cit note 6 at 538, and 543-546; and The Committee on Intellectual Property Rights and the Emerging Information Infrastructure - see National Research Council *The Digital Dilemma: Intellectual Property in the Information Age* (2000) at 222. For a discussion of the >other legitimate reason= proposal, see also Pete Singer >Mounting a Fair Use Defense to the Anti-Circumvention Provisions of the Digital Millennium Copyright Act= (2002) 28 *University of Dayton Law Review* 111 at 140.

<sup>9</sup> Kamiel J Koelman >The Protection of Technological Measures vs. the Copyright Limitations=, paper presented at the ALAI Congress *Adjuncts and Alternatives for Copyright*, New York, 15 June 2001, accessible at <<http://www.ivir.nl/publications/koelman/alaiNY.html>> (visited 3 April 2007).

<sup>10</sup> Besek op cit note 2 at 394.

<sup>11</sup> Koelman op cit note 9.

>Fair use by design= refers to situations where the ability to take advantage of copyright exceptions is built into the technological protection measure. Fair use by design, then, permits spontaneous and anonymous uses.<sup>12</sup>

Section 1201(k) of the United States Copyright Act<sup>13</sup> is an example of this approach. In terms of this paragraph, the copy control measure mandated for analogue videotapes may not preclude copying of free broadcast television or basic cable programming.<sup>14</sup>

Also, in Europe, article 6.4 of the Copyright Directive<sup>15</sup> likewise adopts a fair use by design approach. It seems as if one of the voluntary measures contemplated in article 6.4 is the limited ability to copy. Measures employed by authors that allow a limited number of private copies are deemed legally sufficient to satisfy the private copying privilege. Member States need not provide a private copying privilege, and may do so only with compensation payable to authors. Even if their laws include such a privilege, Member States are not required to ensure that authors provide the means to enable private copying. The fair use by design approach of the Directive does not extend to works made available through on-demand services, nor does it require authors to make the means available for users to exercise their private copying privilege.<sup>16</sup>

Other systems incorporating fair use by design include music download systems, which permit users to play and download songs, usually to multiple computers and playback devices; compact disc copy protection that prevents users from uploading songs to file-sharing sites but allows them to make copies for personal use; and databases that have restrictions on initial access but not persistent controls that preclude copying and forwarding the material retrieved.<sup>17</sup>

Fair use by design has inherent limitations: fair use is not limited to specific categories of

---

<sup>12</sup> Besek op cit note 2 491-492.

<sup>13</sup> 17 USC ' 1201(k).

<sup>14</sup> Besek op cit note 2 at 493.

<sup>15</sup> Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society.

<sup>16</sup> Besek op cit note 2 at 492.

<sup>17</sup> Idem at 493-494.

works or individuals; and authors would likely be unwilling to provide keys for certain types of use, such as parody. Fair use by design provides, at best, rough justice: in some instances users will be technologically restricted from making use that would qualify as fair, whereas, in other instances, they may technologically be empowered to make use that would not qualify as fair.<sup>18</sup>

>Fair use by mandate=, in turn, refers to circumstances in which authors are directed to enable non-infringing uses but not necessarily given specific instructions as to how this should be done.<sup>19</sup>

An example of a fair use by mandate model can be found in article 6.4 of the Copyright Directive. Member States are required to take steps to ensure that the beneficiaries of certain copyright exceptions that allow them lawful access to a copyright work can take advantage of those privileges, but only if authors fail to take >voluntary measures= to do so. Once again, like fair use by design, this approach extends only to certain privileges (not all) and it does not apply to on-demand services. The Directive does not prescribe or limit the technological means that an author may implement to enable the exercise of copyright exceptions. Nor is it limited to technological means: it also contemplates the possibility that such measures may be agreements between authors and the other parties involved.

## 2.4 The Infringement Criterion

As I have shown, it has been suggested that the prohibition on the circumvention of technological protection measures should be limited to circumvention that results in copyright infringement. This will limit the prohibition to instances where such circumvention leads to copyright infringement. So circumvention should be prohibited only where either the *aim* or *effect* of circumvention is infringement.<sup>20</sup>

---

<sup>18</sup> *Idem* at 493.

<sup>19</sup> *Idem* at 492.

<sup>20</sup> Jacqueline Lipton >Copyright in the Digital Age: A Comparative Survey= (2001) 27 *Rutgers Computer and Technology Law Journal* 333 at 361.

In Canada, the *Government Statement on Proposals for Copyright Reforms*<sup>21</sup> states the following regarding the prohibition on circumvention:

>In conformity with the WCT . . . , the circumvention, *for infringing purposes*, of technological measures (TPMs) applied to copyright material would itself constitute an infringement of copyright. Copyright would also be infringed by persons who, for infringing purposes, enable or facilitate circumvention or who, without authorization, distribute copyright material from which TPMs have been removed. It would not be legal to circumvent, without authorization, a TPM applied to a sound recording, notwithstanding the exception for private copying= (emphasis added).

The Canadian Government, then, also advocates an infringement criterion for its proposed implementation of article 11 of the WCT. Only in relation to sound recordings would a circumvention as such be unlawful, irrespective of whether the subsequent action constituted copyright infringement.

It has also been suggested that, in national law, where the prohibition on devices stands, such prohibition should be linked to an infringement criterion. Vinje<sup>22</sup> believes that the United States Congress should, rather than enact a series of exceptions, subject the device prohibition to a general infringement criterion. This will address the problem that lawful users may be unable to circumvent for lawful purposes, as the devices they need for such circumvention are prohibited.

According to Van Coppenhagen,<sup>23</sup> legal protection could be provided against the manufacture and distribution of devices which (a) are promoted, advertised or marketed to circumvent, where it is reasonably foreseeable that such circumvention is for purposes of infringement; (b) have only a limited commercially significant purpose or use other than to circumvent, where it is reasonably foreseeable that such circumvention is to facilitate

---

<sup>21</sup> *Government Statement on Proposals for Copyright Reform*, accessible at

<<http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/en/rp01142e.html>> (visited 27 March 2005).

<sup>22</sup> Thomas Vinje >Copyright Imperilled= [1999] *European Intellectual Property Review* 192 at 199 and 205.

<sup>23</sup> Vanessa van Coppenhagen >Copyright and the WIPO Copyright Treaty, with Specific Reference to the Rights Applicable in a Digital Environment and the Protection of Technological Measures= (2002) 119 *South African Law Journal* 429-452 at 450.

infringing acts; or (c) are primarily designed, produced, adapted, or performed for the purposes of enabling or facilitating circumvention, where it is reasonably foreseeable that such circumvention is for the purposes of infringement.

This may place some obligation on the manufacturer of circumvention devices, or the trafficker in them, to monitor the use of these devices. An infringing purpose may always be foreseeable, because the nature of copyright is such that the same act in respect of the same work may sometimes be lawful, and at times be unlawful. A manufacturer or trafficker would then have to show why an infringing purpose was not reasonably foreseeable in the circumstances.<sup>24</sup>

However, according to Koelman,<sup>25</sup> authors would not gain much if circumvention were to be unlawful only when it is followed by copyright infringement. In those circumstances an author would already have an action for copyright infringement. The action for circumvention would be redundant.

## **2.5 A Knowledge Requirement**

In all instances of indirect copyright infringement, knowledge of the infringement is a requirement for liability. By adding a knowledge requirement to the prohibition on the trafficking in circumvention devices, such trafficking would be treated like indirect copyright infringement. So a person manufacturing, trading in, or selling a circumvention device will be liable only if she actually knew that the device was being used for infringement purposes. In terms of this suggestion, then, it is not the manufacture, trading in, or selling of a circumvention device that is prohibited - performing these acts for non-infringing uses is lawful. Rather, it is the act of trafficking in the device with the knowledge that it will further copyright infringement that is prohibited.

Pennisi,<sup>26</sup> with reference to *Sklyarov* case,<sup>27</sup> states that in cases of criminal circumvention, the

---

<sup>24</sup> *Idem* at 450-451.

<sup>25</sup> Koelman *op cit* note 1 at 279.

<sup>26</sup> Chris Pennisi >Anti-Circumvention Law May Circumvent Fairness= (2002) 19 *Computer and Internet Lawyer* 5-9 at 7-8.

State should be required to prove that the trafficker either knew, or reasonably should have known, that the distribution of the technology would enable significant copyright infringement by any third party. The knowledge requirement, then, would relate not to the dealing with circumvention devices, but to copyright infringement. As Pennisi rightly observes, the current absolute prohibition on devices ignores the fact that no criminal liability exists for the distribution of other instruments useful in the commission of traditional copyright infringement. He accordingly proposes<sup>28</sup> that the prohibition on devices would be far more reasonable if knowledge that the device would be used to enable significant copyright infringement by a third party were required on the part of the violator.

## **2.6 Regulated circumvention devices**

This approach entails the regulation of the manner in which users can obtain circumvention devices, and requires keeping record of the identities of users who seek these devices.<sup>29</sup>

This is the approach currently followed in Australia,<sup>30</sup> for example. It allows users who are >qualified persons= to obtain circumvention devices or services. These users must first supply a declaration that includes their names and addresses; the basis on which they claim to be a >qualified person=; the name and address of the supplier, a statement that the device will be used only for a permitted purpose; and a specific identification of that purpose by reference to the relevant provision in copyright law. This exemption does not cover all user privileges: it is restricted to reverse engineering, and certain uses by libraries, archives, educational institutions, and the State.

In the United States of America, a related suggestion was that a regulatory approach to the provision of circumvention devices should be modelled on federal gun control laws.<sup>31</sup> But is

---

<sup>27</sup> *Department of Justice, Indictment US v Elcom and Dmitry Sklyarov* Criminal No 5-01-257P (ND Cal Filed 2001). See further >Panel III: Implications of Enforcing the Digital Millennium Copyright Act: A Case Study, Focussing on United States v. Sklyarov= (2002) 12 *Fordham Intellectual Property, Media and Entertainment Law Journal* 805 at 806n2.

<sup>28</sup> Pennisi op cit note 26 at 8.

<sup>29</sup> For a full discussion, see Besek op cit note 2 at 489-491.

<sup>30</sup> Section 116A(3) of the Copyright Amendment (Digital Agenda) Act 110 of 2000.

<sup>31</sup> The National Firearms Act of 1934; The Federal Firearms Act of 1938; The Gun Control Act of 1968; The

the gun control model successful enough to warrant serving as a model for dealing with circumvention devices? Even if authorized gun dealers comply with the legislative restrictions, subsequent transfers undermine the system. The same may apply if a similar system were to be adopted for circumvention devices. Also, this suggestion covers only hardware devices and face-to-face transactions, which is unlikely to satisfy those who seek a broad exemption for devices to enable fair use.<sup>32</sup>

Circumvention devices can be effectively regulated only by collecting and maintaining information about the identity of the putative fair user. But this could impinge on user's privacy rights. So it has been suggested that the keys for fair use be held by a trusted third party. Users who want to exercise a fair use privilege would apply for and obtain a key. The trusted third party would then keep record of the keys to protect user privacy, and the identity of users would be revealed only pursuant to a court order and a showing of actual piracy. Each key should be so unique that copies made using it could be traced to it.<sup>33</sup> Casellati<sup>34</sup> believes that the Library of Congress would be the most appropriate agent to hold these keys.

Besek<sup>35</sup> objects to this model. In the first instance, it would not limit unauthorized access or use, because the keys could be obtained by asking for it. Secondly, circumvention would be reduced from an independent claim to an aggravated infringement cause of action. The key access mechanism would merely facilitate proof of the aggravated nature of the offence. Thirdly, unless there is an enforceable means of restricting transfer of the keys, they serve no useful purpose.

All these systems to regulate circumvention devices involve start-up and management costs. They do not provide an effective barrier to infringement. Rather, they merely make it easier to identify infringers.<sup>36</sup>

---

Brady Act of 1993; The Violent Crime Control and Law Enforcement Act of 1994; and The Domestic Violence Offender Gun Ban of 1996.

<sup>32</sup> Besek op cit note 2 at 490.

<sup>33</sup> Idem at 491; and Alvis Maria Casellati >The Evolution of Article 6.4 of the European Information Society Copyright Directive= (2001) 24 *Columbia-VLA Journal of Law & The Arts* 369 at 398.

<sup>34</sup> Casellati op cit note 33 at 398.

<sup>35</sup> Besek op cit note 2 at 491.

## 2.7 Agreements / Licences

When one looks at the importance of agreements in the digital context (such as article 6.4(3) of the Copyright Directive), and the strength of these contractual agreements, it is viable that contractual agreements be implemented to safeguard authors' rights and user privileges. But these agreements should be regulated strictly so that they do not favour authors and allow them contractually to exclude copyright exceptions.

A further possibility may be the introduction of a licensing arrangement in terms of which the manufacturer or trader may manufacture or trade in devices only where she is licensed to do so. It might be a condition of the license that the manufacturer or trader is obliged to monitor the use of the devices that she manufactures or in which she trades.<sup>37</sup>

In Australia, the author has a legal remedy against the person who provides circumvention devices or services. However, exceptions are provided in favour of a manufacturer or trader >where the circumvention device or service is used for a permitted purpose=. These permitted purpose exceptions are defined by reference to specific exceptions in the Australian Copyright Act of 1968.<sup>38</sup>

To ensure that the circumventing device or service is actually used for an authorized purpose, the person wishing to make use of the circumventing device must sign a declaration stating that it will be used only for a permitted purpose. The declaration is also required to contain other information such as the person's name and address, the basis on which she is qualified to use the circumventing device, the name and address of the supplier, the identification of the permitted use by reference to one or more of sections 47D, 47E, 47F, 48A, 49, 50, 51A and 183 and Part VB of the Australian Copyright Act, and a statement that the work in relation to which the device or service is required is not readily available in a form not protected by a technological protection measure.<sup>39</sup>

---

<sup>36</sup> Ibid.

<sup>37</sup> Van Coppenhagen op cit note 23 at 451.

<sup>38</sup> Section 116A(7) of the Copyright Act.

<sup>39</sup> Ibid.

## 2.8 Reasonableness or proof of damages

Pennisi<sup>40</sup> advocates a reasonableness requirement. He argues that civil suits for a violation of the device prohibition could be restricted in scope by forcing the plaintiff to prove that the circumvention at issue enables copyright infringement of a certain threshold monetary value. Basically, he proposes that a plaintiff should prove damage above a certain threshold.

Proof of damage is not required for copyright infringement. But this does seem like a good solution to protect circumvention devices for legitimate uses. Devices causing economic harm would still be targeted, but not devices that enable fair use but not large-scale copying.

## 2.9 Levies

Besek<sup>41</sup> refers to this suggestion, the proponents of which believe that the Audio Recording Act (AHRA)<sup>42</sup> offers a desirable alternative model to the approach adopted in the Copyright Act.

Under the AHRA, (a) all digital audio recording devices are required to implement serial copy management systems (SCMS), a technology that allows an unlimited number of first generation copies but no second generation copies; (b) a levy is imposed on the sale of digital audio recording devices and media, for the benefit of the authors of sound recordings and musical compositions; and (c) consumers are given immunity from copyright infringement suits with respect to certain non-commercial copying of musical recordings.<sup>43</sup>

Proponents of this model argue that the ability to make unlimited first generation copies accommodates fair use and other copyright exceptions and thus reduces the burden on free speech. However, as Besek<sup>44</sup> rightly remarks, it is unclear how first generation copying only would facilitate the exercise of copyright exceptions. If a copy uploaded on the Internet is

---

<sup>40</sup> Pennisi op cit note 26 at 7-8.

<sup>41</sup> For a complete discussion, see Besek op cit note 2 at 485-489.

<sup>42</sup> 17 USC ' 1002(a) and (c).

<sup>43</sup> 17 USC ' ' 1004-06.

<sup>44</sup> Besek op cit note 2 at 486.

regarded as a first generation copy, users would not be able to download it or copy it further. If the copy on the Internet is regarded as the original, users can download it, but any further copying (even for fair use) would be precluded by the technological protection measures preventing second generation copying.

She<sup>45</sup> also refers to the argument that the AHRA approach is more effective because its technology mandate to equipment manufacturers ensures broader coverage than the Copyright Act, while its implementation of a single, specific technology allows Congress to achieve a better balance between authors= and users= interests.

However, it is doubtful that a model requiring a specific mandated technology is preferable as a substitute for the more flexible approach of the Copyright Act (which contains a mandate only in respect of video tape recorders (VTRs)) and protects a wide range of devices. Such a flexible approach, of course, also encourages innovation and experimentation, and allows authors to implement different levels of protection according to their needs and market requirements.<sup>46</sup>

The specific technologies and narrow definitions of the AHRA made it by any accounts a failure, because of the rapid advancement in technology after its passage. I do not think it advisable to follow a similar approach.

With regards to AHRA-like levies, a state administered rewards system for films and sound recordings had been proposed. Revenue would be derived from taxes and distributed to authors in accordance to the frequency with which their works are used. In exchange, users can enjoy these works without payment.<sup>47</sup>

Another proposal is for a >non-commercial use levy=. This levy would be used to compensate authors for unauthorized peer-to-peer file sharing of their works. It would be assessed on Internet access, consumer electronic devices used to copy, download, or store copyrighted materials, and storage media. In exchange users would have immunity from

---

<sup>45</sup> Ibid.

<sup>46</sup> Idem at 487.

copyright infringement suits for non-commercial copying, distribution, performance, or even adaptation of copyright works. The compensation of authors would be based on the frequency of access, and online service providers would collect the access data.<sup>48</sup>

Besek,<sup>49</sup> however, believes that levies should be considered only as a last resort because of the many problems they pose. The first problem is to determine the amount of such levy. Secondly, the collection and allocation of levies would be complicated and costly, as can be seen from the administration of existing compulsory licenses. Thirdly, a levy scheme that would replace exclusive rights with a compulsory license system would be in violation of international treaties. Fourthly, such a levy system would substitute an exclusive right with a right of remuneration, which would require a fundamental alteration to copyright law.<sup>50</sup>

## **2.10 Alternative Business Models**

The suggestion was also made that the circumvention prohibitions should be replaced by alternative business models employed by authors.<sup>51</sup> Besek<sup>52</sup> identifies two problems with these alternative business models. In the first instance, these suggestions contain no specific detail on how new business models can meet consumer expectations and still provide a return sufficient to warrant investment. Secondly, even new business models may need technological protection measures to ensure that authorized users alone benefit from these models.

## **2.11 Intermediary / Collecting Society Model**

This model suggests the establishment of an intermediary that would act as >gatekeeper= for access to circumvention services or devices, which could be made available for use on an appropriate showing.<sup>53</sup>

---

<sup>47</sup> Ibid.

<sup>48</sup> Idem at 487-488.

<sup>49</sup> Idem at 488.

<sup>50</sup> Ibid.

<sup>51</sup> Besek op cit note 2 at 478.

<sup>52</sup> Ibid.

<sup>53</sup> Idem at 494.

In some respects this model is similar to the regulated circumvention devices model. However, it provides greater control since the devices themselves do not circulate.<sup>54</sup>

The problem with this model is to determine the exact extent of the role of the intermediary: should it be purely administrative? Or should the intermediary have the responsibility to make judgements concerning the merits of the claim to a copyright exception?<sup>55</sup>

A middle road was followed in Australia where the intermediary was given some limited screening responsibility. The supplier of circumvention devices and services will supply such devices or services only after a declaration including identification, statement of qualified status, and the specific exception relied on is supplied.<sup>56</sup> Presumably, a responsible intermediary will ensure that the declaration meets the statutory requirements before supplying the devices or services.<sup>57</sup>

Although such an intermediary model may discourage infringing use, it may well also discourage legitimate use. Again such a system will involve financial cost and will discourage spontaneous use and anonymous speech.<sup>58</sup>

### **3 Recommendations for the Implementation of Article 11 of the WCT in South Africa**

#### **3.1 Should South Africa Implement Article 11?**

Sun<sup>59</sup> suggests that developing countries that have not ratified the WCT should think carefully before they do so. If they do, they should avail themselves of the flexibilities inherent in the WCT to maintain the copyright balance, especially mindful of the impact of stronger copyright protection standards on their economic, social, cultural, and technological

---

<sup>54</sup> Ibid.

<sup>55</sup> Ibid.

<sup>56</sup> Section 116A(3) of the Copyright Act.

<sup>57</sup> Besek op cit note 2 at 495.

<sup>58</sup> Idem at 496.

<sup>59</sup> Haochen Sun >Copyright Law Under Siege: An Inquiry into the Legitimacy of Copyright Protection in the Context of the Global Digital Divide= (2005) 36 *ICC* 192 at 211-212.

development.<sup>60</sup>

Also, especially in respect of the prohibition of dealing with circumvention devices, they should consider the alternative remedies that may be available under the law of delict, generally, and the law of unlawful competition, especially.<sup>61</sup>

It goes without saying, too, that developing countries have a special interest in preserving a robust and extensive public domain that encourages the free flow of information and knowledge in order to bridge the knowledge (and digital) divide.<sup>62</sup>

Whether South Africa should implement article 11 is a moot question, because, as I explained in Chapter 7, the Electronic Communications and Transactions Act<sup>63</sup> effectively (perhaps unwittingly) implements article 11 absolutely and without exception.

### **3.2 Exclude the Operation of the Electronic Communications and Transactions Act**

Section 86 of the ECT Act also applies to works protected by copyright. Unfortunately, as I have shown, its provisions are severely detrimental for users of protected works.

The ECT Act provides for the possibility of excluding certain laws from its application. In particular, section 4(3) states the following: >The sections of this Act mentioned in Column B of Schedule 1 do not apply to the laws mentioned in Column A of that Schedule.=

The Copyright Act should accordingly be added to the list of statutes in Column A of Schedule 1, and sections 85-89 in Column B.

The effect of this amendment would be to exclude copyright works from the anti-circumvention provisions of Chapter XIII of the ECT Act.

---

<sup>60</sup> Ibid.

<sup>61</sup> Idem at 212.

<sup>62</sup> Ibid.

<sup>63</sup> Act 25 of 2002 (the >ECT Act=).

### **3.3 Amend the Copyright Act**

A series of consequential amendments should then be made to the Copyright Act.

#### **3.3.1 Definitions**

The following definition should be inserted in section 1(1) of the Copyright Act:

>Atechnological protection measure@ 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 protected by copyright, which are not authorized by the owner of the copyright or permitted by this Act....=

The final phrase of this definition is especially important in that it preserves the current exceptions in sections 12 to 19B of the Act: if a technological protection measure is designed to prevent or restrict excepted acts, it falls outside the ambit of the definition of a >technological protection measure= for the purposes of the Act, and so is not met by the circumvention prohibition.

#### **3.3.2 The Circumvention Prohibition**

The Copyright Act should further be amended with the insertion of a new section 28B, headed >Circumvention of technological protection measures=. I propose that this new provision should read as follows:

- >(1) No person shall, during the subsistence of the copyright in a work and without the licence of the owner of the copyright in such work, knowingly or having reasonable grounds to know, circumvent an effective technological protection measure applied by the owner of the copyright to such work.
- >(2) A technological protection measure shall be deemed to be effective where the use of the work is controlled by the owner of the copyright in it through the

application of an access control or protection process, such as encryption, scrambling, or other transformation of the work, or a copy control mechanism, which achieves the protection objective.

- >(3) Liability under subsection (1) shall be separate and distinct from liability arising under section 23; provided that only for the purposes of section 24, liability under subsection (1) shall be deemed to be copyright infringement under section 23..
- >(4) Nothing in subsection (1) enlarges or diminishes liability for vicarious or contributory copyright infringement in connection with any technology, product, service, device, component, or part of it.=

The application of this prohibition on circumvention is limited to the circumvention of technological protection measures applied to copyright works. This addresses, in particular, the concern that works in the public domain can be >locked up= by technological protection measures.

Liability for unauthorized circumvention is separate and distinct from liability for copyright infringement.

### **3.3.3 Exceptions**

Given the limited scope of both the definition of a >technological protection measure= and of the circumvention prohibition, I propose that only exceptions for *(a)* certain actions of non-profit libraries or archives, and educational institutions; *(b)* reverse engineering; and *(c)* law enforcement.

To this end, I propose that the following subsections be added to the proposed section 28A:

- >(5) A non-profit library or archive, or an educational institution, which, by engaging in conduct set out in subsection (1), gains access to a work

protected by copyright solely in order to make a good faith determination as to whether to acquire a copy of such work shall not be in violation of subsection (1); provided that a copy of a work to which access has been obtained under this subsection -

- (a) may not be retained longer than necessary to make such a good faith determination; and
- (b) may not be used for any other purpose.

>(6) Notwithstanding the provisions of subsection (1), a person who has lawfully obtained the right to use a computer program may circumvent a technological protection measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analysing those elements of the program necessary to achieve the interoperability of an independently created computer program with other computer programs, and that have not previously been readily available to the person engaging in the circumvention, to the extent that any such acts of identification and analysis do not constitute an infringement of copyright under section 23.

>(7) The provisions of subsection (1) shall not prohibit the circumvention of a technological protection measure for any lawfully authorized investigative, protective, or intelligence activity by an agent, employee, or officer of the State.=

Finally, I propose a new section 28A(8), modelled on section 13, which allows the Minister to create further exceptions by way of regulations, to be published in the *Government Gazette*:

- >(8) In addition to the circumvention of technological protection measures permitted in terms of this Act, circumvention of a technological protection measures shall also be permitted as prescribed by the Minister by regulation, after due consideration of the following factors:
- (a) the availability for use of works protected by copyright;

- (b) the availability for use of works for non-profit archival and educational purposes;
- (c) the impact of the prohibition on the circumvention of technological protection measures applied to works protected by copyright on criticism, comment, news reporting, teaching, scholarship, or research;
- (d) the effect of the circumvention of technological protection measures on the market for or value of works protected by copyright; and
- (e) such other factors as the Minister considers appropriate.=

#### **4 A Final Teaser**

Which way should South Africa go? It depends, said the Cheshire Cat, a great deal on where we want to get. Do we want to provide stronger protection for authors, so risking widening the digital divide between ourselves as a country of the South and the countries of the North, or do we want to ensure managed and reasonable access to protected copyright works and a vibrant public domain?

## Bibliography

### BOOKS AND CHAPTERS IN BOOKS

- John Perry Barlow 'Selling Wine Without Bottles. The Economy of Mind on the Global Net' in P. Bernt Hugenholtz (ed.) *The Future of Copyright in a Digital Environment* 1996 London: Kluwer Law International 169-187
- Jonathan Burchell *Principles of Criminal Law* 2005 Juta and Company Ltd
- Charles Clark 'The Answer to the Machine is in the Machine' in P. Bernt Hugenholtz (ed.) *The Future of Copyright in a Digital Environment* 1996 London: Kluwer Law International 139-146
- William Cornish & David Llewellyn *Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights* 5 ed London: Sweet & Maxwell
- OH Dean *Handbook of South African Copyright Law* (loose-leaf, revision service 12, 2004)
- GE Devenish 'Constitutional Law' in *LAWSA* Vol 5(3) 2ed (2004)
- Mihály Ficsor *The Law of Copyright and the Internet: The 1996 WIPO Treaties, their interpretation and Implementation* 2002 Oxford University Press
- Jonathan Griffiths and Uma Suthersanen (editors) *Copyright and Free Speech Comparative and International Analyses* 2006 Oxford University Press
- Lucie M.C.R. Guibault *Copyright Limitations and Contracts: An Analysis of the Contractual Overridability of Limitations on Copyright* Doctoral Thesis, 2002 Amsterdam
- Michael Lehmann 'Digitisation and Copyright Agreements' Dr Irini A. Stamatoudi and Paul L.C. Torremans (ed) in *Perspectives on Intellectual Property: Copyright in the New Digital Environment* 2000 London: Sweet & Maxwell 195-203
- Jessica Litman *Digital Copyright* 2001 Prometheus Books
- National Research Council *The Digital Dilemma: Intellectual Property in the Information Age* 2000 National Academy Press
- Dorothy Schrader 'Digital Millennium Copyright Act, P.L. 105-304: Summary and Analysis' in John V Martin (ed) *Copyright: Current Issues and Laws* 2002 New York: Nova Science Publishers
- CR Snyman *Strafreg* 2006 Durban: Lexisnexis Butterworths

### JOURNALS

- Carolyn Andrepont 'Digital Millennium Copyright Act: Copyright Protections for the Digital Age' (1999) 9 *De Paul-LCA Journal of Art and Entertainment Law* 397-420
- Christopher Arup 'The US-Australia FTA: law making on the frontier' (2004) 29 *Alternative Law Journal* 27-34
- Jonathan Band 'The Digital Millennium Copyright Act: A Balanced Result' [1999] *European Intellectual Property Review* 92-94
- Jonathan Band & Taro Isshiki 'The New US Anti-Circumvention Provision: Heading in the Wrong Direction' (1999) 15 *Computer Law & Security Report* 219-225
- June M Besek 'Anti-Circumvention Laws and Copyright: A Report from the Kernochan Center for Law, Media and the Arts' (2004) 27 *Columbia Journal of Law & the Arts* 385-519
- Cynthia M Botte 'Protection of Information Products: Balancing Commercial Reality and the Public Domain' (1998) 67 *University of Cincinnati Law Review* 237-264

Angela Bowne 'Trade Marks and Copyright on the Internet' (1997) 2 *Media and Arts Law Review* 135

Kathy Bowrey 'Who's Writing Copyright's History?' [1996] *European Intellectual Property Review* 322-329

Denis T Brogan 'Fair Use no Longer: How the Digital Millennium Copyright Act Bars Fair Use of Digitally Stored Copyrighted Works' (2002) 16 *St John's Journal of Legal Commentary* 691-725

Lee A. Bygrave 'The Technologicalisation of Copyright: Implications for Privacy and Related Interests' [2002] *European Intellectual Property Review* 51-57

Alvise Maria Casellati 'The Evolution of Article 6.4 of the European Information Society Copyright Directive' (2001) 24 *Columbia-VLA Journal of Law & The Arts* 369-402

Tamber Christian 'Implementation of the WIPO Copyright Treaty - How Hard Can it Be?' (1998) 15 *Computer Lawyer* 8-16

Andrew Christie 'Reconceptualising Copyright in the Digital Era' [1995] *European Intellectual Property Review* 522-530

Julie E Cohen 'WIPO Copyright Treaty Implementation in the United States: Will Fair Use Survive?' [1999] *European Intellectual Property Review* 236-247

Committee on Intellectual Property Rights and the Emerging Information Infrastructure; Computer Science and Telecommunications Board; Commission on Physical Sciences, Mathematics, and Applications; National Research Council 'The Digital Dilemma: Intellectual Property in the Information Age' (2001) 62 *Ohio State Law Journal* 951-971

Stephen J. Davidson, Scott J. Berg, and Michael Kapsner 'Open, Click, Download, Send - To What Have You Agreed?' (2001) 4 *Journal of Internet Law* 1-14

G Gervaise Davis III 'The Digital Dilemma: Coping with Copyright in a Digital World' (1993) 27 *Copyright World* 18-26

OH Dean 'The Case for the Recognition of Intellectual Property in the Bill of Rights' (1997) 60 *Tydskrif vir die Hedendaagse Romeins Hollandse Reg* 105-119.

Allen N. Dixon & Martin F. Hansen 'The Berne Convention Enters the Digital Age' [1996] *European Intellectual Property Review* 604-612

Allen N. Dixon & Laurie C. Self 'Copyright Protection for the Information Superhighway' [1994] *European Intellectual Property Review* 465-472

Michael Doherty & Ivor Griffiths 'The Harmonisation of European Union Copyright Law for the Digital Age' [2000] *European Intellectual Property Review* 17-23

Thomas K. Dreier 'Convergence Through Digital Technology - The Effect on Copyright and Information Services' 10<sup>th</sup> Annual Conference on Intellectual Property Law and Policy, 5 April 2002 1-13

Thomas Dreier 'Unsolved copyright issues in the digital and network environment' (1995) 48 *Copyright World* 36-40

S verine Dusollier 'Exceptions and Technological Measures in the European Copyright Directive of 2001 - An Empty Promise' (2003) 34 *ICC* 62-75

Mark Felsenthal & Angela Droite 'Administration Outlines Objectives for Global Internet Policy' (1997) 14(28) *International Trade Reporter (BNA)* 1179

Ralph Fischer 'The Expansion of Intellectual Property Rights by International Agreement: A Case Study Comparing Chile and Australia's Bilateral FTA Negotiations With the U.S' (2006) 28 *Loyola of Los Angeles International and Comparative Law Review* 129-70

Dr Mihály Fiscor 'The Spring 1997 Horace S. Manges Lecture - Copyright for the Digital Era: The WIPO "Internet" Treaties' (1997) 21 *Columbia - VLA Journal of Law and the Arts* 197-223

Simon Fitzpatrick 'Copyright Imbalance: U.S. and Australian Responses to the WIPO Digital Copyright Treaty' [2000] *European Intellectual Property Review* 214-228

Eric Fleischmann 'The Impact of Digital Technology on Copyright Law' (1988) 70 *Journal of Patent and Trademark Office* 5-26

David Fletcher 'Brave New eWorld - What Lessons can the ePublishing Industry Learn from the Music Industry?' (2000) 105 *Copyright World* 9-10

David Flint 'Encryption - Plainly Free Speech?' (2000) 102 *Copyright World* 19-21

Christophe Geiger 'Right to Copy v. Three-Step Test The Future of the Private Copy Exception in the Digital Environment' (2005) 1 *CRi* 7-13

Jane C. Ginsberg 'Copyright Legislation for the "Digital Millennium"' (1999) 23 *Columbia - VLA Journal of Law and the Arts* 137-179

Jane C Ginsberg 'Copyright Use and Excuse on the Internet' (2000) 24 *Columbia-VLA Journal of Law & The Arts* 1-45

David Goldberg & Robert J Bernstein 'The Prohibition on Circumvention and the Attack on the DVD' [2001] *European Intellectual Property Review* 160-163

Derrick Grover 'Data Watermarking: Steganography and Watermarking of Digital Data' (2001) 17 *Computer Law & Security Report* 101-104

Nick Hanbidge 'DRM: Can It Deliver?' (2001) 12 *Entertainment Law Review* 138-140

Nick Hanbidge 'Protecting Rights Holders' Interests in the Information Society: Anti-circumvention; Threats Post-Napster; and DRM' (2001) 12 *Entertainment Law Review* 223-225

Michael Hart 'The Copyright in the Information Society Directive: An Overview' [2002] *European Intellectual Property Review* 58-64

P. Bernt Hugenholtz 'Why the Copyright Directive is Unimportant, and Possibly Invalid' [2000] *European Intellectual Property Review* 499-505

Christine Jeanneret 'The Digital Millennium Copyright Act: Preserving the Traditional Copyright Balance' (2001) 12 *Fordham Intellectual Property, Media and Entertainment Law Journal* 157-194

David R. Johnson and David Post 'Law and Borders - The Rise of Cyberlaw' (1996) 48 *Stanford Law Review* 1367-1402

Eric D Keller 'Scan Now, Pay Later: Copyright Infringement in Digital Document Storage' (2000) 26 *The Journal of Corporation Law* 177-198

Gabriela Kennedy 'Copyright in the Information Society: A World of More Copies and Rights' (1999) 93 *Copyright World* 15-20

Gabriela Kennedy 'Encryption Policies: Codemakers, Codebrakers and Rulemakers: Dilemmas in Current Encryption Policies' (2000) 16 *Computer Law & Security Report* 240-247

Melissa A. Kern 'Paradigm Shifts and Access Controls: An Economic Analysis of the Anticircumvention Provisions of the Digital Millennium Copyright Act' (2002) 35 *University of Michigan Journal of Law Reform* 891-935

Selena Kim 'The Reinforcement of International Copyright for the Digital Age' (2002) 16 *Intellectual Property Journal* 93-122

Kamiel J. Koelman 'A Hard Nut to Crack: The Protection of Technological Measures' [2000] *European Intellectual Property Review* 272-280

Stephen M. Kramarsky 'Copyright Enforcement In the Internet Age: The Law and Technology of Digital Rights Management' (2001) 11 *De Paul - LCA Journal of Art and Entertainment Law* 1-43

Peter Kumik 'Digital Rights Management' (2001) 1 *Legal Information Management* 21-23

LA Kurtz 'Copyright and the National Information Infrastructure in the United States' [1996] *European Intellectual Property Review* 120-126

Mr Justice Laddie 'Copyright: Over-strength, Over-regulated, Over-rated?' [1996] *European Intellectual Property Review* 253-260

Michael Landau 'Digital Downloads, Copy Code, and U.S. Copyright Law' 9<sup>th</sup> *Annual Conference on Intellectual Property Law and Policy*, New York, 19 April 2001, 1-24

Euan Lawson and Andre Steed 'Sounds Unlimited 2: Music and Copyright in Cyberspace - An Update' (1999) 90 *Copyright World* 16-21

Brian Leubitz 'Digital Millennium? Technological Protections for Copyright on the Internet' (2003) 11 *Texas Intellectual Property Law Journal* 417-446

Jacqueline Lipton 'Copyright in the Digital Age: A Comparative Survey' (2001) 27 *Rutgers Computer & Technology Law Journal* 333-369

Andre Lucas 'Copyright Law and Technical Protection Devices' (1997) 21 *Columbia - VLA Journal of Law and the Arts* 225-238

Gregory C Ludlow 'Copyright and the Challenge of the Digital World' (1999) 3 *Canadian International Lawyer* 199-206

Glynn S Lunney Jr 'The Death of Copyright: Digital Technology, Private Copying and the Digital Millennium Copyright Act' (2001) 87 *Virginia Law Review* 813-920

Andrew Manning and John Selby 'A Fine Line Between Legal Access and Circumvention: The Australian High Court Provides a pyrrhic victory for the sale of mod-chips' (2005) *CRi* 161-165

Dean S. Marks & Bruce H. Turnbull 'Technical Protection Measures: The Intersection of Technology, Law and Commercial Licences' [2000] *European Intellectual Property Review* 198-213

Alex Morrison & Lorna E. Gillies 'Securing Webcast Content in the European Union: Copyright, Technical Protection and Problems of Jurisdiction on the Internet' [2000] *European Intellectual Property Review* 74-80

Susan A Mort 'The WTO, WIPO & the Internet: Confounding the Borders of Copyright and Neighboring Rights' (1997) 8 *Fordham Intellectual Property, Media and Entertainment Law Journal* 173-221

Karen Murray 'The Draft Directive on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society' (1998) 9 *Entertainment Law Review* 190-192

David Nimmer 'A Riff on Fair Use in the Digital Millennium Copyright Act' (2000) 148 *University of Pennsylvania Law Review* 673-742

David Nimmer 'A Tale of Two Treaties Dateline: Geneva - December 1996' (1997) 22 *Columbia - VLA Journal of Law and the Arts* 1-25

David Nimmer 'Back From the Future: A Proleptic Review of the Digital Millennium Copyright Act' (2001) 16 *Berkeley Technology Law Journal* 855-876

David Nimmer 'Time and Space' (1998) 38 *IDEA: The Journal of Law and Technology* 501-527

'Panel III: Implications of Enforcing the Digital Millennium Copyright Act: A Case Study, Focussing on United States v. Sklyarov' (2002) 12 *Fordham Intellectual Property, Media and Entertainment Law Journal* 805-858

Chris Pennisi >Anti-Circumvention Law May Circumvent Fairness= (2002) 19  
*Computer and Internet Lawyer* 5-9

T Pistorius 'The Enforceability of Shrink Wrap Agreements in South Africa' (1993) 5  
*South African Mercantile Law Journal* 1-19

David Price 'Fighting Fire with Fire: Monitoring Intellectual Property in a Digital Age' (2001) 111 *Copyright World* 14-15

Patrick Ravillard 'Towards a European Directive on Enforcement of Intellectual Property Rights' (2001) 136 *Trademark World* 40-44

Jörg Reinbothe & Silke von Lewinski 'The WIPO Treaties 1996: Ready to Come into Force' [2002] *European Intellectual Property Review* 199-208

M.T. Michéle Rennie 'E.U. Copyright Directive: May 1999 Amendments to Appease Some Industry Sectors' (1999) 5 *Computer and Telecommunications Law Review* 123-126

Heather Rosenblatt 'Protocol to the Berne Convention The WIPO Diplomatic Conference - the Birth of Two New Treaties' (1997) 13 *The Computer Law & Security Report* 307-311

Werner Rumphorst 'Fine-tuning Copyright for the Information Society' [1996] *European Intellectual Property Review* 79-82

Tricia J Sadd 'Fair Use as a Defense under the Digital Millennium Copyright Act's Anti-Circumvention Provisions' (2001) 10 *George Mason Law Review* 321-344

Pamela Samuelson 'Comparing U.S. and E.C. Copyright Protection for Computer Programs: Are They more Different than They Seem?' (1994) 13 *Journal of Law and Commerce* 279.

Pamela Samuelson 'Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised' (1999) 14 *Berkeley Technology Law Journal* 519-566

Pamela Samuelson 'The U.S. Digital Agenda at WIPO' (1997) 37 *Virginia Journal of International Law* 369-439

Jason Sheets 'Copyright Misused: The Impact of the DMCA Anti-circumvention Measures on Fair & Innovative Markets' (2000) 23 *Hastings Communications and Entertainment Law Journal* 1-27

Pete Singer 'Mounting a Fair Use Defense to the Anti-Circumvention Provisions of the Digital Millennium Copyright Act' (2002) 28 *University of Dayton Law Review* 111-142

Graham J H Smith 'The Future of Intellectual Property in an Online World' (1996) 7 *Computers and Law* 33-37

JAL Sterling 'Philosophical and Legal Challenges in the Context of Copyright and Digital Technology' (2000) 31 *International Review of Industrial Property and Copyright Law* 508

Haochen Sun 'Copyright Law Under Siege: An Inquiry into the Legitimacy of Copyright Protection in the Context of the Global Digital Divide' (2005) 36 *ICC* 192-213

John Tessenhohn 'A New Dawn in the Japanese Fight against Digital Piracy' (1999) 10 *Entertainment Law Review* 186-188

Vanessa van Copenhagen 'Copyright and the WIPO Copyright Treaty, with Specific Reference to the Rights Available in a Digital Environment and the Protection of Technological Measures' (2002) 119 *South African Law Journal* 429-452

Ryan L. Van Den Elzen 'Decrypting the DMCA: Fair Use as a Defense to the Distribution of DeCSS' (2002) 77 *The Notre Dame Law Review* 673-704

Coen van Laer 'Open Forum: The New European Copyright Directive' (2001) 29 *International Journal of Legal Information* xlvii- xlix

Dana van der Merwe 'Computer crime - recent national and international developments' (2003) 66 *Tydskrif vir Hedendaagse Romeins Hollandse Reg* 30-44

T.C.Vinje 'A Brave New World of Technical Protection Systems: Will There Still be Room for Copyright?' [1996] *European Intellectual Property Review* 431-440

Thomas C. Vinje 'All's Not Quiet on the Berne Front' [1996] *European Intellectual Property Review* 585-589

Thomas Vinje 'Copyright Imperilled?' [1999] *European Intellectual Property Review* 192-207

Coenraad Visser 'Online Service Provider Liability under the Electronic Communications and Transactions Act 25 of 2002' (2002) 14 *South African Mercantile LJ* 758-764

Silke von Lewinski 'A Successful Step towards Copyright and Related Rights in the Information Age: The New E.C. Proposal for a Harmonisation Directive' [1998] *European Intellectual Property Review* 135-139

Silke von Lewinski 'Proposed EC Directive on Copyright and Related Rights in the Information Society as It Progresses' (1999) 30 *ICC* 767-782

David N Weiskopf 'The Risks of Copyright Infringement on the Internet: A Practitioner's Guide' (1998) 33 *University of San Francisco Law Review* 1-58

Jonathan Weinberg 'Digital TV, Copy Control, and Public Policy' (2002) 20 *Cardozo Arts and Entertainment Law Journal* 277-294

Wend Wendland 'The Digital Agenda' (1997) 5 *Juta's Business Law* 143

Raquel Xalabarder 'Copyright: Choice of Law and Jurisdiction in the Digital Age' (2002) 8 *Annual Survey of International and Comparative Law* 79-96

Alfred C Yen 'Restoring the Natural Law: Copyright as Labor and Possession' (1990) 51 *Ohio State Law Journal* 517-559

## INTERNET

<[http://europa.eu.int/documents/comm/index\\_en.htm](http://europa.eu.int/documents/comm/index_en.htm)> (visited on 11 March 2004). OJ L89/6 11/4/2000 accessible at

<[http://europa.eu.int/comm/internal\\_market/en/intprop/news/ratification.htm](http://europa.eu.int/comm/internal_market/en/intprop/news/ratification.htm)> (visited on 5 May 2002)

<[http://europa.eu.int/comm/internal\\_market/en/intprop/news/ratification.htm](http://europa.eu.int/comm/internal_market/en/intprop/news/ratification.htm)> (visited on 5 April 2002)

<<http://eurorights.org/eudmca/>> (visited on 20 March 2002)

<<http://www.ifpi.org/site-content/library/wipo%20treaties%20-%20technical%20measures.pdf>> (visited on 5 April 2002)

<<http://www.nationmedia.com/eastafrican/current/News/News2606200619.htm>> (visited on 28 June 2006)

<<http://www.wipo.int/pressroom/en/releases/2002/p304.htm>> (visited on 2002-03-14)

<[http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty\\_id=16](http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=16)> (visited on 11 January 2007)

<[http://www.wipo.int/treaties/en/Remarks.jsp?cnty\\_id=1525C](http://www.wipo.int/treaties/en/Remarks.jsp?cnty_id=1525C)> (visited on 27 April 2005)

A Quick look at the Uniform Computer Information Transactions Act accessible at <<http://www.arl.org/info/frn/copy/ucita.html>> (visited on 21 November 2006)

<[http://www.bambooweb.com/articles/u/n/Uniform\\_Computer\\_Information\\_Transactions\\_Act.html](http://www.bambooweb.com/articles/u/n/Uniform_Computer_Information_Transactions_Act.html)> (visited on 28 February 2005)

Edward Barrow 'Rights clearance and technical protection in an electronic environment' accessible at <<http://associnst.ox.ac.uk/~icsuinfo/barrow.htm>> (visited on 20 March 2002)

Mark Bide, Charles Oppenheim and Anne Ramsden 'Copyright Clearance and Digitization in UK Higher Education: Supporting Study for the JISC/PA Clearance Mechanisms Working Party' accessible at <<http://www.ukoln.ac.uk/services/elib/papers/pa/clearance/>> (visited on 21 November 2006)

<[http://civies.com/content/agents/2b\\_agent.htm](http://civies.com/content/agents/2b_agent.htm)> (visited on 28 February 2005)

Roger Clarke 'Technological Protections for Digital Copyright Object' accessible at <<http://www.anu.edu.au/people/Roger.Clarke/II/TPDCO.html>> (visited on 22 November 2006)

'The Digital Millennium Copyright Act of 1998: U.S. Copyright Office Summary', accessible at <<http://www.loc.gov/copyright/legislation/dmca.pdf>> (visited on 18 March 2002)

'Digital Technology and the Copyright Act 1994: A Discussion Paper - Part Two: Background' accessible at <[http://www.med.govt.nz/buslt/int\\_prop/digital/digital-04.html](http://www.med.govt.nz/buslt/int_prop/digital/digital-04.html)> (visited on 3 October 2002)

Thomas Dreier 'Copyright Law and Digital Exploitation of Works' accessible at <<http://www.fes.de/fulltext/stabsabteilung/00218001.htm>> (visited on 3 October 2002)

Séverine Dusollier 'Situating legal protections for copyright-related technological measures in the broader legal landscape: ANTI CIRCUMVENTION PROTECTION OUTSIDE COPYRIGHT' *General Report I.C. ALAI 2001 Congress, New York, June 13-17* accessible at <[http://www.law.columbia.edu/conferences/2001/3\\_reports-en.htm](http://www.law.columbia.edu/conferences/2001/3_reports-en.htm)> (visited on 30 September 2002)

Electronic Frontier Foundation 'Security Researchers Drop Scientific Censorship Case', accessible at <[http://www.eff.org/IP/DMCA/Felten\\_v\\_RIAA/20020206\\_eff\\_felten\\_pr.html](http://www.eff.org/IP/DMCA/Felten_v_RIAA/20020206_eff_felten_pr.html)> (last visited on 5 May 2002)

*Government Statement on Proposals for Copyright Reform*, accessible at <<http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/en/rp01142e.html>> (visited 27 March 2005)

Laurence R Helfer 'Regime Shifting: The Trips Agreement and New Dynamics of International Intellectual Property Lawmaking' accessible at <<http://www.law.vanderbilt.edu/faculty/faculty-directory/laurence-r-helfer/download.aspx?id=649>> (visited on 29 January 2007)

Institute of Information Law, Amsterdam 'Protection of Technological Measures' *November 1998* accessible at <<http://www.imprimatur.net/IMP-FTP/technical.pdf>> (visited on 27 June 2002)

Kamiel J. Koelman 'The protection of technological measures vs. the copyright limitations' paper presented at the *ALAI Congress Adjuncts and Alternatives for Copyright*, New York, 15 June 2001 accessible at <<http://www.ivir.nl/publications/koelman/alaiNY.html>> (visited on 3 April 2007)

Joe Kraus, Testimony to the House Energy and Commerce Committee (Apr. 25, 2002), accessible at <<http://www.digitalconsumer.org/testimony-20020425.html>> (visited on 20 March 2007)

J. Litman 'Digital Copyright and Information Policy' accessible at <<http://www-personal.umich.edu/~7Ejdlitman/papers/casrip.html>> (visited on 21 November 2006)

'Report to Congress: Joint Study of Section 1201(g) of the Digital Millennium Copyright Act' accessible at [http://www.loc.gov/copyright/reports/studies/dmca\\_report.html](http://www.loc.gov/copyright/reports/studies/dmca_report.html) (visited on 15 February 2007)

Report of the Digital Opportunity Task Force (DOT Force), "Digital Opportunities for All: Meeting the Challenge" 6 (2001), accessible at <http://www.g8.utoronto.ca/summit/2001genoa/dotforce1.html> (last visited on 8 February 2006)

Pamela Samuelson 'On Authors' Rights in Cyberspace: Questioning the Need for New International Rules on Authors' Rights in Cyberspace' accessible at <http://www.firstmonday.dk/issues/issue4/samuelson/> (visited on 21 November 2006)

SCADPlus *Green Paper on Copyright and Related Rights in the Information Society* accessible at <http://europa.eu.int/scadplus/leg/en/lvb/124152.htm> (visited on 11 March 2004)

Neil A Smith 'Supreme Court Report: Metro-Goldwyn-Mayer Studios Inc et al v Grokster Ltd et al 125 S.Ct. 2764 (2005)' accessible at <http://www.sheppardmullin.com/images/pubs/pub502.pdf> (visited on 26 June 2006)

<http://www.tralac.org/scripts/content.php?id=4774> (visited on 28 June 2006).

'UCITA: Uniform Computer Information Transactions Act' accessible at <http://www.jameshuggins.com/h/tek1/ucita.htm> (visited on 21 November 2006)

'U.S. Copyright Office – Statement of the Librarian of Congress Relating to Section 1201 Rulemaking', accessible at [http://www.copyright.gov/1201/docs/librarian\\_statement\\_01.html](http://www.copyright.gov/1201/docs/librarian_statement_01.html) (visited on 2 March 2004)

Charlotte Waelde 'The Quest for Access in the Digital Era: Copyright and the Internet' (2001) 1 *The Journal of Information, Law and Technology* accessible at <http://elj.warwick.ac.uk/jilt/01-1/waelde.html> (WT/DS160/R of 15 June 2000)

accessible at [http://wto.org/english/tratop\\_e/dispu\\_e/1234da.pdf](http://wto.org/english/tratop_e/dispu_e/1234da.pdf) (visited on 28 March 2007)

## TABLE OF OFFICIAL DOCUMENTS

### **International Conventions and Documents**

Agreed Statements on the provisions of the WCT

Agreement on Trade-Related Aspects of Intellectual Property Rights (the TRIPS Agreement)

Amendments to Articles 7, 10, 13 and 14 of Draft Treaty N° 1 proposed by the Delegations of Algeria, Angola, Burkina Faso, Cameroon, Chad, Côte d'Ivoire, Egypt, Ethiopia, Gabon, Gambia, Ghana, Kenya, Lesotho, Libya, Madagascar, Malawi, Mali, Mauritius, Morocco, Namibia, Niger, Nigeria, Senegal, South Africa, Sudan, Togo, Tunisia, United Republic of Tanzania, Zambia and Zimbabwe, WIPO Document CRNR/DC/56, 12 December 1996

Basic Proposal on the Substantive Provisions of the Treaty on Certain Questions Concerning the Protection of Literary and Artistic Works to be Considered by the Diplomatic Conference, WIPO Doc. CRNR/DC/4 (Aug 30, 1996).

The Customs Union Agreement between South Africa, Botswana, Lesotho, Namibia and Swaziland of 21 October 2002.

Berne Convention for the Protection of Literary and Artistic Works (Paris Act 1971)  
Proposals Submitted by the United States of America to the Committee of Experts on a Possible Protocol to the Berne Convention, Sixth Session, Geneva, 1 to 9 February 1996

Universal Declaration of Human Rights, Adopted and proclaimed by General Assembly resolution 217 A (III) of 10 December 1948

WIPO Copyright Treaty (the WCT)

WIPO Phonograms and Performances Treaty (the WPPT)

WIPO, Questions Concerning a Possible Protocol to the Berne Convention: Proposal of Argentina, BCP/CE/V/7 (6 September 1995).

### **United States of America**

Audio Home Recording Act 17 USC § 1002(C)

Communications Act 47 USC §605

Computer Fraud and Abuse Act 18 U.S.C

Consumer Broadband and Digital TV Promotion Act of 2002 S. 2048, 107th Congress, 2d Session.

Consumers, Schools and Libraries Digital Rights Management Awareness Act of 2003, S 1621, 108th Congress (2003).

Copyright Act 17 U.S.C

Digital Media Consumers' Rights Act of 2003 HR 107, 108th Congress., 1st Sess. (2003)

Digital Millennium Copyright Act L No 105-304, 112 Stat 2860 (28 October 1998).

Electronic Communications Privacy Act (the "Federal Wiretap Act") 18 U.S.C

House Judiciary Report on the DMCA H.R.Rep.No. 105-551

Information Infrastructure Task Force Intellectual Property and the National Information Infrastructure: *A Preliminary Draft of the Report of the Working Group on Intellectual Property Rights: The Green Paper* (July 1994)

Information Infrastructure Task Force: *The Report of the Working Group on Intellectual Property Rights, Intellectual Property and the National Information Infrastructure: The White Paper* (Sept 1995) (jointly referred to as the 'US White Paper Bill')

No Electronic Theft Act of 1997 Codified in scattered sections of 17 and 18 USC.

North American Free Trade Agreement (NAFTA) 32 I.L.M

Sonny Bono Copyright Term Extension Act, Pub. L. No. 105-298, 112 Stat. 2827 (1998)

S.2037, 105th Cong (1998) (the 'Hatch Bill')

Stored Wire and Electronic Communications Act 18 U.S.C

Uniform Commercial Code

Uniform Computer Information Transactions Act 1999: Draft for Approval

Uniform Trade Secrets Act

United States Constitution

Wire Fraud Act 18 USC § 1343

### **European Union**

Amended Proposal for a European Parliament and Council Directive on the harmonisation of certain aspects of copyrights and related rights in the Information Society COM(1999)250/FINAL  
Communication from the Commission to the Council and the European Parliament and to the Economic and Social Committee and the Committee of Regions, COM(94)347/FINAL  
Council Common Position on 28 September 2000 [2000] O.J. C344/1  
Council Directive 91/250/EEC of 14 May 1991 on the Legal Protection of Computer Programs  
Council Directive 92/100/EEC of 19 November 1992 on the Rental Right and Lending Right and on Certain Rights Related to Copyright in the Field of Intellectual Property  
Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts  
Council Directive 93/83/EEC of 27 September 1993 on the Co-ordination of Certain Rules Concerning Copyright and Rights Related to Copyright Applicable to Satellite Broadcasting and Cable Retransmission  
Council Directive 93/98/EEC of 29 October 1993 on Harmonizing the Term of Protection of Copyright and Certain Related Rights  
Directive 95/46 /EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data  
Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the Protection of Consumers in Respect of Distance Contracts  
Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, and consisting of, conditional access  
Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases  
Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society  
Follow-up Paper to the Green Paper on Copyright and Related Rights in the Information Society COM(1996)568  
Green Paper on Copyright and Related Rights in the Information Society COM(1995)382/FINAL  
Proposal for a European Parliament and Council Directive on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society COM(97)628/FINAL

### **South Africa**

Constitution of the Republic of South Africa, Act 108 of 1996  
Copyright Act 98 of 1978  
Electronic Communications and Transactions Act 25 of 2002  
Promotion of Access to Information Act 2 of 2000  
South African Law Commission's proposed Data Protection and Privacy Act, October 2005

### **United Kingdom**

Computer Misuse Act 1990  
Copyright, Designs and Patents Act 1988

## **Australia**

Australia-United States Free Trade Agreement  
Australian Copyright Act of 1968  
US Free Trade Agreement Implementation Act 120 of 2004

## TABLE OF CASES

### **United States of America**

*321 Studios v Metro Goldwyn Mayer Studios INC et al*, 307 F.Supp.2d 1085 (N.D.Cal. 2004)  
*A&M Records Inc v Napster Inc* 239 F 3d 1004 (9th Cir 2001)  
*Cable/Home Communications Corp v Network Productions Inc* 902 F 2d 829 (11th Cir 1990)  
*The Chamberlain Group Inc v Skylink Technologies Inc* (N.D. Ill. unreported civil action No 02 C 6376)  
*CSC Holdings v. Greenleaf Electronics*, 2000 U.S. Dist. LEXIS 7675 (N.D. Ill. 2000)  
*Department of Justice, Indictment US v Elcom and Dmitry Sklyarov* Criminal No 5-01-257P (ND Cal Filed 2001)  
*Diamond v Am-Law Publishing Corp* 745 F 2d 142 (2d Cir 1984)  
*Harper & Row, Publishers, Inc. v. Nation Enters.*, 471 U.S. 539 (1985)  
*IMS Inquiry Management Systems Ltd v Berkshire Information Systems* 307 F. Supp. 2d 521 (S.D.N.Y. 2004)  
*Lexmark International Inc v Static Control Components Inc.*, 253 F Supp 2d 943 (ED Ky 2003)  
*Mazer v Stein* 347 US 201 (1954)  
*Metro-Goldwyn-Mayer Studios Inc v Grokster* 125 S Ct 2764 (2005)  
*Millar v Taylor* (1769) 4 Burr 2303  
*Paramount Pictures Corporation and Twentieth Century Fox Film Corporation v 321 Sega Enterprises Ltd v Accolade Inc* 977 F.2d 1510 (9th Cir 1992)  
*Paramount Pictures Corporation and Twentieth Century Fox Film Corporation v 321 Studios, a/k/a 321 Studios LLC, a/k/a Terr Lcc*, No 03-CV-8970 RO (SDNY 2004)  
*Pearl Investments LLC v Standard I/O Inc Pearl Investments LLC v Standard I/O Inc* 257 F.Supp. 2d 326 (D.Me. 2003)  
*ProCD Inc v Zeidenberg* 86 F. 3d 1447 (7<sup>th</sup> Cir. 1996)  
*Quinto v Legal Times of Washington Inc* 511 F Supp 579 (DDC 1981)  
*Realnetworks Inc v Streambox Inc.* No C99-207OP, 2000 US Dist LEXIS 1889 (WDWash)  
*Sony Computer Entertainment America Inc v Gamemasters*, 87 F.Supp. 2d 976 (N.D. Cal. 1999).  
*Sony Corp of Am v Universal City Studios Inc* 464 US 417 (1984)  
*United States v Elcom Ltd*, 203 F.Supp. 2d 1111 (N.D.Cal. 2002)  
*Universal City Studios, Inc v Corley* 272 F.3d 429, 444 (2nd Cir. 2001).  
*Universal City Studios Inc v Reimerdes*: 111 F.Supp. 2d 294 (S.N.D.Y. 2000).  
*Universal City Studios Inc v Reimerdes* 82 F.Supp. 2d 211 (S.D.N.Y. 2000)

## **South Africa**

*Atari Inc & another v JB Radio Parts (Pty) Ltd* (TPD (case no 17419/83) unreported)  
*August v Electoral Commission* 1999 4 BCLR 363 (CC); 1999 3 SA 1 (CC)  
*Bosal Africa (Pty) Ltd v Grapnel (Pty) Ltd & another* 1985 (4) SA 882 (C)  
*Christian Education South Africa v Minister of Education* 2000 10 BCLR 1051 (CC);  
2000 4 SA 757 (CC)  
*Dawoo v Minister of Home Affairs, Shalabi v Minister of Home Affairs, Thomas v  
McKenzie v Van der Merwe* 1917 AD 41 at 51.  
*Minister of Home Affairs* 2000 8 BCLR 837 (CC); 2000 3 sa 936 (CC).  
*Ex parte Chairperson of the Constitutional Assembly: In re Certification of the  
Constitution of the Republic of South Africa, 1996* 1996 (4) SA 744 (CC)  
*Galago Publishers (Pty)Ltd & another v Erasmus* 1989 (1) SA 276 (A)  
*Khala v Minister of Safety & Security* 1994 2 BCLR 89 (W); 1994 4 SA 218 (W)  
*S v Makwanyane* 1995 6 BCLR 665 (CC); 1995 3 SA 391 (CC); 1995 2 SACR 1 (CC)

## **Australia**

*Stevens v Kabushiki Kaisha Computer Entertainment*, [2005] HCA 58 (6 October  
2005)

## Index

|  |  |
|--|--|
| access control .....                           | 29, 73, 109  |
| initial access control .....                   | 30   |
| receiver-end access control .....              | 30   |
| subsequent access control .....                | 30   |
| access right .....                             | 240, 245, 258  |
| access right in the analogue environment ..... | 243  |
| access right in the digital environment .....  | 244  |
| act of circumvention .....                     | 100, 190, 273, 289, 91, 102, 104, 109, 112, 131, 146, 152, 156, 159, 161, 174, 177, 178, 182, 190, 191, 192, 194, 195, 198, 201, 220, 221, 232, 235, 252, 273  |
| agreements .....                               | 24, 26, 38, 53, 195, 199, 205, 206, 210, 282   |
| alternative business models .....              | 285  |
| anti-intellectual property response .....      | 43   |
| authenticity protection .....                  | 34   |
| broadcasting .....                             | 202  |
| choice of law .....                            | 19, 215  |
| circumvention devices ....                     | 55, 63, 70, 71, 80, 87, 89, 92, 97, 102, 109, 110, 112, 131, 137, 141, 144, 147, 148, 157, 159, 162, 172, 174, 179, 183, 185, 188, 192, 193, 195, 198, 211, 220, 221, 232, 233, 235, 252, 269, 273, 275, 279, 280, 281, 282, 283, 286, 287 |
| click wrap contracts .....                     | 24   |
| collecting society model .....                 | 286  |
| constitutional rights .....                    | 227, 229, 254  |
| contract .....                                 | 24, 25, 26, 36, 37, 42, 74, 141, 201, 205, 206, 209, 212, 213, 214, 215, 218, 220, 221, 241, 264, 265, 282   |
| contributory liability .....                   | 232  |
| copy control .....                             | 29, 31, 32, 33, 35, 73, 94, 97, 100, 101, 109, 112, 113, 114, 115, 137, 144, 163, 184, 188, 192, 201, 235, 244, 247, 249, 251, 253, 276, 289   |
| copyright balance ....                         | 21, 26, 57, 60, 72, 135, 138, 165, 215, 220, 223, 231, 237, 272, 273, 287  |
| developing countries .....                     | 223, 224, 226, 227, 228, 236, 238, 287   |
| digital divide .....                           | 223, 224, 225, 228, 291  |
| digital lockup .....                           | 155, 156   |
| digitization .....                             | 5  |
| and developing countries .....                 | 223  |
| impact on economic rights .....                | 12   |
| impact on enforcement of rights .....          | 17   |
| impact on format of works .....                | 6  |
| impact on moral rights .....                   | 15   |
| impact on uses of works .....                  | 7  |
| impact on distribution of works .....          | 9  |
| rights of authors .....                        | 12   |
| direct infringement .....                      | 231  |
| disabilities .....                             | 203, 204   |
| economic rights .....                          | 12, 166  |
| reproduction .....                             | 13   |
| distribution .....                             | 14   |
| electronic contract .....                      | 25, 215, 221, 222  |

|  |  |
|--|--|
| encryption .....                           | 28, 29, 32, 39, 40, 98, 110, 113, 146, 188, 253, 264, 289  |
| encryption research .....                  | 118, 132, 133, 145, 146, 147, 148, 151, 152, 158   |
| enforcement of rights .....                | 17, 77, 153  |
| enforcement of judgements .....            | 21   |
| ephemeral recordings .....                 | 202  |
| equipment manufacturers .....              | 114, 195   |
| exceptions .....                           | 140, 197, 199, 220, 274, 290   |
| fair use .....                             | 44, 57, 58, 60, 75, 89, 95, 105, 107, 110, 112, 115, 123, 130, 133, 134, 135, 136, 137, 138, 139, 140, 156, 159, 161, 162, 163, 190, 207, 242, 259, 263, 267, 268, 269, 276, 277, 281, 283, 284                          |
| fair use by design .....                   | 276  |
| first sale doctrine .....                  | 157, 158, 265,   |
| free trade agreements .....                | 56, 225, 236, 266  |
| gun control .....                          | 281  |
| harmonization of copyright laws .....      | 220  |
| illustration .....                         | 203  |
| infringement criterion .....               | 231, 277   |
| integrity protection .....                 | 34   |
| intellectual property response .....       | 45   |
| intermediary .....                         | 252, 286   |
| knowledge requirement .....                | 57, 60, 64, 74, 177, 182, 191, 256, 257, 279   |
| limitations ... ..                         | 22, 44, 57, 75, 76, 81, 87, 117, 133, 134, 136, 140, 148, 174, 180, 182, 183, 188, 190, 191, 195, 198, 199, 200, 201, 204, 205, 206, 210, 220, 227, 228, 229, 231, 237, 259, 265, 266, 267, 269, 272, 273, 274, 275, 277 |
| law enforcement .....                      | 95, 141, 290   |
| levies .....                               | 115, 283, 285  |
| library .....                              | 67, 95, 120, 122, 140, 153, 155, 202, 207, 270, 290  |
| licenses .....                             | 25, 33, 34, 38, 158, 262, 263, 264, 282, 285   |
| minors .....                               | 95, 120, 148, 149  |
| monitoring .....                           | 118, 119, 196, 197   |
| rule-making .....                          | 118, 120, 121, 124   |
| study concerning encryption research ..... | 132  |
| monopoly .....                             | 85, 117, 160, 179, 186, 198, 221   |
| moral rights .....                         | 15, 53, 166  |
| right of attribution .....                 | 15   |
| right of integrity .....                   | 16   |
| non-infringing use ... ..                  | 65, 66, 87, 90, 94, 101, 104, 105, 107, 113, 117, 118, 119, 122, 123, 124, 125, 130, 131, 156, 157, 160, 161, 163, 164, 197, 275, 277, 279   |
| obligations of authors .....               | 87, 97, 116, 195   |
| payment-per-use .....                      | 157, 260   |
| physical embodiment .....                  | 240, 241, 242, 243, 246, 261, 263, 264   |
| platform shifting .....                    | 265  |
| privacy .....                              | 18, 30, 70, 150, 151, 174, 192, 248, 260, 261, 281   |
| private copying .....                      | 184, 185, 196, 207, 208, 209, 210, 211, 267, 276, 278  |
| proof of damages .....                     | 283  |
| public domain ....                         | 21, 22, 24, 58, 62, 63, 67, 68, 90, 91, 107, 108, 156, 171, 226, 227, 228  |
| public security .....                      | 204  |
| reasonableness .....                       | 283  |
| remedies ..                                | 39, 61, 67, 68, 69, 70, 75, 77, 78, 79, 80, 87, 92, 104, 133, 135, 136,  |

|  |               |
|--|---------------|
| 153, 204, 218, 233, 254, 257, 282, 287   |               |
| replacement parts .....  | 159           |
| repography .....   | 202           |
| reverse engineering ... 59, 95, 141, 142, 143, 144, 145, 158, 190, 216, 218, 220, 280, 290 |               |
| rights management information .....  | 33            |
| right to demand access .....   | 266           |
| rule-making .....  | 118           |
| initial .....  | 120           |
| second .....   | 121           |
| third .....  | 124           |
| savings clauses .....  | 133, 197      |
| security testing .....   | 151, 152, 153 |
| shrink wrap contract .....   | 24            |
| technological protection .....   | 26            |
| usage metering .....   | 36            |