

Copyright:  
Law and Practice in a Digital Age

Honours Thesis

School of Information Technology and Electrical Engineering  
The University of Queensland

David Starkoff  
33439055

Supervisors:

Dr. Cristina Cifuentes  
Dr. Anne Fitzgerald

## Abstract

Copyright law is a branch of intellectual property which protects the expressions of ideas. Computer programs are protected by copyright law as literary works; the holder of the copyright in a computer program can control all reproductions of it unless expressly allowed by law.

The extent to which copyright can regulate the behaviour of computer programs is first detailed. As very little can be done with a computer program without reproducing it, this protection is pervasive. Non-infringing uses of computer software in the United States, Australia and the European Union are described.

Complementary to the protection of computer software is the protection of computer data. The effect of the World Intellectual Property Organisation Copyright Treaty (an international treaty), the Digital Millennium Copyright Act (United States legislation), the *Copyright Amendment (Digital Agenda) Act 2000* (Australian legislation) and Directive 2001/29/EC (European Union legislation) is explicated.

Building upon the preceding understanding of the extent copyright law, copyright law is then applied to four separate common behaviours in computer science: reverse engineering, peer-to-peer networking, technological protection measures and academic research. The extent of the legal protection is then critiqued and improvements to the law suggested.

The thesis concludes with suggestions for remedial action and future research directions.

### **A note to the reader about referencing**

This thesis concerns two different disciplines: computer science and law. The thesis is primarily intended for a computer science audience, although readers with legal training should be able to identify the authority for legal propositions with precision.

Computer scientists and legal scholars use different systems of referencing. Computer scientists use single references to entries in a bibliography which is at the end of a work; lawyers tend to use footnotes and references to a specific point inside a work.

To reconcile this difference I have adopted the approach used by journals such as the *Communications of the ACM* when publishing legal articles intended for a computer science audience. Articles, books and other like sources familiar to computer scientists are contained in a bibliography at the end of the thesis. Citations and references to such works in the text are contained by a number in square brackets. Legislation, cases and other such legal references are contained in footnotes at the bottom of each page.

Legal referencing has been done, as far as possible, in accordance with the style mandated by the T. C. Beirne School of Law at The University of Queensland [92]. References to United States authorities conform with [7].

### **Acknowledgements**

This thesis would not have been possible without the patience and guidance of my supervisors, Dr. Cristina Cifuentes and Dr. Anne Fitzgerald. Their insights and understanding of the topic area enlivened my research (and provided a welcome pretext for a Californian stopover in October). All deficiencies and errors in this thesis should be attributed to my inadequacy rather than their supervision.

A tip o' the hat is also due to the crew in room 523, in particular Mike Van Emmerik and Sasitharan Balasubramaniam for putting up with my presence over the course of the year.

Finally, no acknowledgements page would be complete without loving thanks to my family, who suffered through various stages of my stress levels on a wholly involuntary basis.

# Contents

<b>1</b>	<b>Introduction</b>	<b>4</b>
1.1	Historical context . . . . .	4
1.2	State of the art . . . . .	6
1.3	Relevance of thesis . . . . .	7
1.4	Overview of contents . . . . .	7
<b>2</b>	<b>Copyright</b>	<b>9</b>
2.1	History . . . . .	9
2.2	Berne Convention . . . . .	10
2.3	Computer programs . . . . .	11
2.3.1	United States . . . . .	11
2.3.2	Australia . . . . .	12
2.3.3	International consensus . . . . .	15
2.4	Software licensing . . . . .	16
2.4.1	Shrink-wraps, click-wraps and browse-wraps . . . . .	16
2.4.2	Terms of licensing . . . . .	18
2.5	Protected uses . . . . .	21
2.5.1	Ordinary course of operation . . . . .	22
2.5.2	Study . . . . .	23
2.5.3	Back-up copies . . . . .	24
2.5.4	Reverse engineering . . . . .	24
2.6	Summary . . . . .	24
<b>3</b>	<b>Protecting computerised data</b>	<b>25</b>
3.1	International treaties . . . . .	25
3.1.1	WIPO Copyright Treaty . . . . .	25
3.1.2	WIPO Performance and Phonograms Treaty . . . . .	28
3.2	United States . . . . .	30
3.2.1	Digital Millennium Copyright Act . . . . .	30
3.2.2	Recent legislative proposals . . . . .	36
3.3	Australia . . . . .	37

3.3.1	Copyright Amendment (Digital Agenda) Act . . . . .	37
3.4	The European Union . . . . .	43
3.5	The United Kingdom . . . . .	44
3.6	Summary . . . . .	45
<b>4</b>	<b>Applying the law to the technology</b>	<b>46</b>
4.1	Reverse engineering . . . . .	46
4.1.1	European Union . . . . .	47
4.1.2	United States . . . . .	47
4.1.3	Australia . . . . .	50
4.2	Peer-to-peer networks . . . . .	62
4.2.1	Napster . . . . .	63
4.2.2	MP3.com . . . . .	65
4.2.3	Other P2P networks . . . . .	66
4.3	Technological protection measures . . . . .	67
4.3.1	Encryption schemes . . . . .	67
4.3.2	Watermarking . . . . .	72
4.3.3	Trusted systems . . . . .	72
4.4	Academic research . . . . .	74
4.4.1	In the United States . . . . .	74
4.4.2	In Australia . . . . .	75
4.4.3	In the European Union . . . . .	75
4.4.4	In the United Kingdom . . . . .	75
<b>5</b>	<b>Analysis</b>	<b>77</b>
5.1	Is copyright the appropriate protection for computer software? . . . . .	77
5.1.1	Patent protection . . . . .	77
5.1.2	<i>Sui generis</i> protection . . . . .	78
5.1.3	Software as speech . . . . .	79
5.2	Could copyright protection for computer programs be improved? . . . . .	80
5.2.1	Subsequent unauthorised use in Australia . . . . .	80
5.2.2	Can the guarantees be side-stepped? . . . . .	81
5.3	Could the circumvention provisions be improved? . . . . .	82
5.3.1	Are they necessary? . . . . .	83
5.3.2	Defining a circumvention device . . . . .	85
5.3.3	Valé fair use and fair dealing? . . . . .	86
5.3.4	Intermediate copies in transit . . . . .	87
5.3.5	Recent legislative developments . . . . .	88
5.4	Should a commons be legislated? . . . . .	89

<b>6 Conclusion</b>	<b>92</b>
6.1 Summary . . . . .	92
6.2 Remedial action . . . . .	92
6.3 Further research . . . . .	93
<b>A International treaty provisions</b>	<b>95</b>
A.1 WIPO Performances and Phonograms Treaty . . . . .	95
<b>B European Union legislation</b>	<b>97</b>
B.1 Directive 91/250/EEC . . . . .	97
B.2 Directive 2001/29/EC . . . . .	106
<b>Bibliography</b>	<b>114</b>

# Chapter 1

## Introduction

Law and computer science have typically and traditionally been disparate, however this separation is no longer appropriate. Copyright law in particular has increasing application to computer science.

### 1.1 Historical context

Computers are not new. Charles Babbage conceived of a mechanical “difference engine” in Victorian England, although the first computer actually made was probably the Turing machines at Bletchely Park during World War II [82]. Computer programs are also not new. Ada Byron, Countess of Lovelace, wrote programs for her colleague (and possibly lover) Babbage’s difference engine [23].

Intellectual property is likewise not new [80]. The doctrine of copyright, for example, can be traced back to a monopoly given to stationers by the Tudor and Stuart monarchs in England. Copyright law in its modern form was internationally agreed upon towards the end of the nineteenth century with the Berne Convention for the Protection of Literary and Artistic Works.

The nexus between computers, computer programs and intellectual property is, however, comparatively new [76]. Only recently has the tension graduated from theoretical concern to popular news. It has

even been suggested that hackers will be the pornographers of the new millennium—pushing the boundaries of First Amendment protection in the United States to the benefit of the public at large [96].

There are numerous reasons for the rise of this tension, including the rise of the personal computer, the ubiquity of the Internet (propelled by the popularity of the World Wide Web) and the rise of digital music (and, to a lesser extent, digital video) as a viable data transfer medium [41]. Within the space of less than a decade, science fiction [39] has become science fact.

Concomitant with the growing popularity and wide appeal of computing technology, government regulation has increased. This has taken the form of legislation reflecting the interests of powerful media conglomerates to the exclusion of previously established checks and balances. The poster child for this movement is the Digital Millennium Copyright Act, passed by the United States Congress in 1998. The criminalization of conduct neither necessary nor sufficient for copyright infringement ignores the rights to which the populace (and especially the computing populace) has become accustomed, and gives well-funded media copyright holders unprecedented power over their works.

The emergence of a dialogue on the appropriate protections for computer programs and computer data is an opportunity to critically evaluate the multitude of purposes for which computers are now used. Politicians and law-makers are still, for the most part, ignorant of issues in the computing community and the computing community can still, for the most part, not persuasively communicate with politicians and regulators. This is something which must change.

My Honours thesis explores the issues underpinning this tension, critically evaluates the legal measures developed in response to the perceived problems and critically evaluates a selection of technological protection measures which can be used to enforce controls on the use and distribution of digital information.

## 1.2 State of the art

There are a number of examples of this tension which will be explored in this thesis. These same examples will be considered in greater detail in Chapter 4.

**Reverse engineering** Reverse engineering is “the process of analysing an existing system to identify its components and interrelationships, to create a representation of the system at a higher level of abstraction” [14]. It is a valuable tool for computer scientists—it is often used to examine interfaces in order to create interoperable products, sometimes in order to identify potential security problems. Copyright law restricts the ability of computer scientists to reverse engineer computer software.

**Peer-to-peer networking** Napster, a peer-to-peer network for the sharing of music files, also attracted legal scrutiny. Copyright law restricts the ability of operators of networks because of the content which they may carry.

**Encryption schemes** Increasingly, digital data is being protected by means of encryption. Examples of this are Digital Video Discs (DVDs) and Adobe eBooks. Publishers of the data use these schemes to control the use of the data, with the protection of copyright law. Circumventing the technological protection schemes may attract civil and criminal liability, regardless of the legality of any subsequent use of the data.

**Trusted systems** In recent times, publishers have investigated the possibility of only distributing data through “trusted” channels—channels where constraints on the use and further distribution of works are enforced. The extent to which these trusted systems are protected under the law is largely a concern of copyright law.

**Academic research** Encryption research and security testing have long been domains of academic research. Academics study implementations, provide critical analyses and publish their findings. This long-standing collegial tradition is under threat due to the operation of copyright law.

### **1.3 Relevance of thesis**

Computer scientists are increasingly subject to the nuances of copyright law; ignorance is no longer bliss. Computing professionals (and computer scientists) often reproduce computer programs for the purposes of studying their behaviour and gleaning the principles of their operation. Oftentimes, reverse engineering is used to create interoperable products, to correct errors or to do security testing. These behaviours are regulated by copyright law to differing extents in different jurisdictions. Even academic research may attract the threat of legal action.

Because of the recent encroachment of copyright law into the realm of day-to-day computer science, an examination of the issues of this thesis is relevant.

### **1.4 Overview of contents**

Chapter 2 introduces the basic concepts of copyright law and details the application of copyright protection to computer software. This chapter, Chapter 3 and Chapter 4 are dispassionate expositions of the state of the law or technology; analysis and criticism is contained in Chapter 5.

Chapter 3 investigates recent changes to copyright laws, largely concerning the protection of digital data. The changes on the international level, in the United States of America and in Australia are identified and analysed.

Chapter 4 discusses the application of copyright law (as detailed in Chapters 2 and 3) to common behaviours of computer scientists and computing professionals.

Chapter 5 critically analyses the protection given to computer programs (as detailed in Chapter 2) and the protection given to computerised data (as detailed in Chapter 3) in light of the applications detailed in Chapter 4.

Chapter 6 concludes the thesis, summarising the findings, suggesting a course of remedial action and suggesting further research topics.

# Chapter 2

## Copyright

As the name “copyright” may imply, copyright is a species of intellectual property rights concerning the reproduction of works. In a doctrinal sense, copyright protects the expression of ideas, not ideas themselves. (For example, copyright protects the text of a Mills & Boon book, but does not protect the basic plot of romance found and experienced.) A copyright holder has a bundle of exclusive rights, including the right to reproduce the work and the right to make adaptations of the work (or derivative works). The copyright holder—initially the author—may assign or license these rights to others.

### 2.1 History

Copyright has a long and storied history. In mediæval England, the Stationers Guild developed a monopoly over the printing of books. The Tudor and Stuart monarchs, as a convenient means of censorship, extended this to cover the importation of books [41, 70]. Members of the Guild, on registration of the work, obtained a perpetual right to publish the work.

With the Glorious Revolution of 1688 and the exile of James II, Parliament, and not the monarch became the ascendant organ of government. The *Statute of Anne* was passed in 1709, granting a limited term (twenty-eight years) of copyright that originally vested in the authors, rather than

printers. The copyright could be subsequently assigned to the printers.

Copyright evolved piecemeal until the end of the nineteenth century. The British Parliament passed an omnibus copyright act, essentially in similar terms to the Berne Convention, which essentially is the form of copyright protection in the world today.

## 2.2 Berne Convention

The Berne Convention for the Protection of Literary and Artistic Works was completed at Paris on 4 May 1896.<sup>1</sup> It established “a Union for the protection of the rights of authors in their literary and artistic works.”<sup>2</sup> Member States of the Union agreed to a base level of intellectual property protections. Under the Berne Convention, copyright protection is automatic. The term of protection granted for literary works is “the life of the author and fifty years after his death.”<sup>3</sup> Authors of literary works are granted the exclusive right to authorise:

- reproduction of their works;<sup>4</sup>
- “adaptations, arrangements and other alterations of their works”,<sup>5</sup> including cinematic adaptations;<sup>6</sup>
- broadcasting, “communication to the public by wire” or “public communication by loudspeaker or any other analogous instrument” of their works;<sup>7</sup> and
- public recitation of their works.<sup>8</sup>

---

<sup>1</sup>The text of the treaty and a list of parties is available at <<http://www.wipo.int/treaties/ip/berne/index.html>>.

<sup>2</sup>Article 1.

<sup>3</sup>Article 7(1).

<sup>4</sup>Article 9(1).

<sup>5</sup>Article 12(1).

<sup>6</sup>Article 14(1).

<sup>7</sup>Article 11*bis*(1).

<sup>8</sup>Article 11*ter*(1).

A treaty is an instrument of international law, not national law. Generally, international treaties become law not when signed or ratified by governments but when (or if) they are implemented domestically. As such, international treaties are not generally a source of law. That is not to say, however, that they are completely irrelevant. It is often in governments' interests to implement treaties in domestic legislation. Principles of international comity play a part, as can the more practical motive of wishing to avoid trade sanctions [42].

In the area of intellectual property, conventions are important. The Berne Convention is widely implemented and reflects the base line of international intellectual property protection. One hundred and forty-eight countries are parties to the Berne Convention: Australia became a member of the Union on 14 April 1928, the United Kingdom on 4 December 1887 and the United States of America on 1 March 1989.

## **2.3 Computer programs**

As computers and computer software became more prevalent during the 1970s, the question arose as to what intellectual property protection applied to computer software. Computer programs in printed-out source code form were certainly literary works: they satisfied the requisite elements of originality and literary value. The logical deduction from this observation was that computer programs in all forms should attract copyright protection as if they were literary works—just the same as novels. This is indeed the approach that was taken (some criticisms of this approach are detailed in Section 5.1).

### **2.3.1 United States**

In the United States, copyright law was consolidated and reformed in 1976 with the passing of the Copyright Act,<sup>9</sup> subsequently codified as Title 17

---

<sup>9</sup>Act of Oct. 19, 1976, Pub. L. No. 94-553, 90 Stat. 2541.

of the United States Code. The legislative history suggested that computer programs were included as literary works.<sup>10</sup> A report commissioned shortly thereafter recommended that the computer programs be explicitly mentioned to remove any doubt as to the applicability of copyright protection to computer programs.<sup>11</sup> Congress adopted the suggestion.<sup>12</sup> (The conclusions and investigations of the report which led, in particular, to the 1980 amendments to the Copyright Act are robustly criticised in [1, 11].)

This general history is recounted in the decision of the Court of Appeals for the Third Circuit in *Apple Computer, Inc. v. Franklin Computer Corporation*.<sup>13</sup> That decision also removed any doubt as to the application of the statute, holding that computer programs in object code, a computer program embedded in a ROM chip and operating systems programs are covered by copyright.<sup>14</sup>

### 2.3.2 Australia

In Australia, the assumption that computer programs would be protected by copyright as literary works prevailed until Apple Computer sued Computer Edge, who imported a “Wombat” computer from Taiwan.<sup>15</sup> The primary substantive difference between a Wombat computer and an Apple II was that “Wombat” appeared in the Wombat machine where “Apple” appeared in the Apple. Indeed, some Wombat computers were sold with an Apple II Reference Manual as their documentation.

Apple asserted their copyright in the object code was breached by the Wombat’s unauthorised reproductions of a substantial part (indeed virtually all) of their ROM code. Computer Edge was accused of indirectly infringing Apple’s copyright by importing infringing devices.<sup>16</sup>

---

<sup>10</sup>H.R. Rep. No. 1476, 94th Cong., 2d Sess. 54.

<sup>11</sup>National Commission on New Technological Uses of Copyrighted Works, *Final Report* 1 (1979).

<sup>12</sup>Act of Dec. 12, 1980, Pub. L. No. 96-517, § 10, 94 Stat. 3015, 3028.

<sup>13</sup>714 F.2d 1240, 1246–48 (3d Cir. 1983).

<sup>14</sup>*Apple Computer*, 714 F.2d at 1249–54.

<sup>15</sup>*Apple Computer Inc v Computer Edge Pty Ltd* (1983) 50 ALR 581.

<sup>16</sup>*Copyright Act 1968* (Cth) ss 38, 39.

At first instance, Apple failed to show that copyright indeed subsisted in the ROM code. In most copyright actions, this element is trivially satisfied; however in this case it was the stumbling block. The ROM code was physically imperceptible by human beings: no person could the information contained in a ROM chip. Justice Beaumont therefore held that no copyright could subsist, and thus there was no copyright infringement.<sup>17</sup>

Justice Beaumont's decision was appealed to the Full Court of the Federal Court of Australia, who upheld the appeal.<sup>18</sup> Computer Edge further appealed the matter to the High Court of Australia where Justice Beaumont's decision was vindicated.<sup>19</sup> The High Court held that the object codes could not be literary works for the purposes of the *Copyright Act*, despite source code being protected as literary works.

The ruling of Justice Beaumont at first instance sent shockwaves through the computer industry in Australia. Pressure was exerted on the Commonwealth Government to ensure that computer programs, no matter their form or how stored, were protected by copyright. Parliament duly obliged and passed the *Copyright Amendment Act 1984* (Cth). The amendment had retrospective effect,<sup>20</sup> although for constitutional reasons it did not affect the dispute between Apple and Computer Edge.<sup>21</sup> Although the amendments were only intended to be a stop-gap measure, they have proved "surprisingly durable" [70].

The amendments to the *Copyright Act* ensured that the High Court's judgment was essentially limited to the dispute between Apple and Computer Edge. It also removed the possibility that similar issues would ever be litigated in Australia.

### **What is a computer program?**

In Australian law, a computer program is<sup>22</sup>

---

<sup>17</sup>(1983) 50 ALR 581 at 591–92.

<sup>18</sup>*Apple Computer Inc v Computer Edge Pty Ltd* (1984) 1 FCR 549; 53 ALR 225.

<sup>19</sup>*Computer Edge Pty Ltd v Apple Computer Inc* (1986) 161 CLR 171.

<sup>20</sup>*Copyright Amendment Act 1984* (Cth) s 7.

<sup>21</sup>*Computer Edge Pty Ltd v Apple Computer Inc* (1986) 161 CLR 171 at 177 per Gibbs CJ.

<sup>22</sup>*Copyright Act 1968* (Cth) s 10(1).

a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result.

The extent of this broad definition fell for consideration in, oddly enough, a tax case.<sup>23</sup> In the case, K Mart purchased music CDs and claimed their contents were exempt from tax as computer programs. The definition of a “computer program” for tax purposes was the same as the definition of a “computer program” in the *Copyright Act*.<sup>24</sup> It was agreed between the parties that a music CD player was a “device having digital information processing capabilities” (used in the *Copyright Act* at that time instead of “computer”).

Justice O’Connor of the Federal Court of Australia noted that “[t]here is no consensus in the computer industry in relation to the general question of ‘what is a computer program?’ as it applies to special purpose computers” (such as CD players).<sup>25</sup> Based on expert evidence from Dr. Jayasooriah from the University of New South Wales, Justice O’Connor adopted a layered approach to computer programs and computer data; holding that the purely audio data “remains . . . passive data without any instructional function” whereas non-audio data (such as framing information) was instructional.<sup>26</sup>

This approach was followed by the High Court of Australia in *Data Access Corporation v Powerflex Services Pty Ltd*.<sup>27</sup> In that case, Data Access argued (*inter alia*) that reserved words in the Dataflex language were themselves computer programs. The High Court did not accept this argument.<sup>28</sup> The reserved words, the Court said, were mnemonic shorthand for the benefit of users. The reserved words themselves, although they may invoke sets of instructions, are not sets of instructions themselves. Indeed, the name of a reserved word had no necessary connection with its

---

<sup>23</sup>*K Mart Australia Ltd v Commissioner of Taxation* (1998) 88 FCR 336.

<sup>24</sup>*Sales Tax Assessment Act 1992* (Cth) s 5.

<sup>25</sup>(1998) 88 FCR 336 at 347.

<sup>26</sup>(1998) 88 FCR 336 at 348.

<sup>27</sup>(1999) 202 CLR 1; 166 ALR 228; 45 IPR 353; [1999] HCA 49 (30 September 1999). The case is further discussed in Section 4.1.

<sup>28</sup>[1999] HCA 49 at 71.

behaviour.

A case currently before the Federal Court of Australia [52] will decide whether DVDs are computer programs or films. Without preempting the decision in the pending case (which should be similar to *K Mart Australia Ltd v Commissioner of Taxation*), it appears then that in Australia a “computer program” for the purpose of copyright law must have some inherent instructional function—purely interpreted data does fall within the definition.

### 2.3.3 International consensus

The Berne Convention was last amended in 1979; the definition of literary and artistic works in Article 2(1) does not expressly include computer programs. Further treaties have addressed this gap, proscribing that computer programs should be protected by copyright law as literary works.

The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) is Annex 1C to the World Trade Organization Agreement. It must be agreed to by any nation wishing to join the WTO. The WTO was established on 1 January 1995; as of 26 July 2001, there were 142 member countries of the WTO.

Regarding computer software, TRIPS reflected the orthodoxy of the time:<sup>29</sup>

Computer programs, whether in source or object code, shall be protected as literary works under the Berne Convention (1971).

The World Intellectual Property Organization Copyright Treaty, completed in 1996, also contains a similar provision:<sup>30</sup>

Computer programs are protected as literary works within the meaning of Article 2 of the Berne Convention. Such protection applies to computer programs, whatever may be the mode or form of their expression.

---

<sup>29</sup>Article 10(1).

<sup>30</sup>Article 4.

Again, this does little beyond recognise the way that computer programs had been dealt with in national law and, indeed, in TRIPS.

## 2.4 Software licensing

The protection of computer programs as literary works is automatic in all Berne Convention countries, requiring no registration or extra effort on the part of the author.<sup>31</sup> As noted in Section 2.2, one of the exclusive rights granted to the author of a literary work is the right to reproduce the work. Without the consent (or license) of the copyright holder, no one can substantially reproduce the copyrighted work.

For computer programs, this is pervasive: the execution, backing up and downloading of computer software all involve the making of reproductions. Many of these necessary reproductions are now expressly protected by copyright legislation; other uses require a license from the author of the software.

Accordingly, a license is the general way that software is distributed. Computer software is rarely sold for several reasons. First, selling computer software involves the copyright holder relinquishing control over the work. Additionally, in the United States, the “first sale doctrine”<sup>32</sup> provides that after the first sale of a copy of a work, the buyer can further sell or dispose of the work as he or she sees fit. This is obviously undesirable for computer software authors, so licensing is the preferred means of retaining control over the copyrighted software.

### 2.4.1 Shrink-wraps, click-wraps and browse-wraps

For bundled, packaged computer software, the computer industry licensed their software by the use of “shrink-wrap” licenses. A consumer went to their software store of preference, exchanged money for a pack-

---

<sup>31</sup>In the United States, although registration is not necessary for copyright to subsist, it is necessary for copyright to be enforced: 17 U.S.C. § 411.

<sup>32</sup>17 U.S.C. § 109.

age containing the software in question, then came home to install it. Enclosed within the shrink-wrapped package was a license (hence the name “shrink-wrap license”). Via a dialog box, or something similar, in the initial installation of the software, the user agreed that they had read the license (another copy may be displayed as part of the installation process). This was accepted by courts as being a binding license.<sup>33</sup>

An extension on this same theme was the so-called “click-wrap” license. These are a feature of online software distribution. With online software, there are no boxes—nothing to shrink-wrap. The user is informed of the software license by displaying the license and forcing the user to manifest their assent to the terms of the license (or “click-through”). The trend of courts in the United States is to accept these licenses as legally binding.<sup>34</sup>

In Australia, the validity of shrink-wrap or click-wrap licensing has not been decided, however copyright notices in a prominent place in distribution is sufficient.<sup>35</sup>

A recent attempted extension to this notion is that of a “browse-wrap” license, where the license terms are pointed to by a link on the download page, or somewhere similar. Licenses like this have only recently been litigated. In the two cases decided in the United States, their validity has been impugned on both occasions.<sup>36</sup> The distinction between the valid click-wrap licenses and invalid browse-wrap licenses is that users did not have to see, let alone agree to, the browse-wrap license’s terms.<sup>37</sup>

---

<sup>33</sup>*Hill v. Gateway 2000, Inc.*, 105 F.3d 1147 (7th Cir. 1997); *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996).

<sup>34</sup>*In re RealNetworks, Inc., Privacy Litigation*, No. 00 C 1366, 2000 U.S. Dist. LEXIS 6584 (N.D. Ill. May, 11, 2000); *Hotmail Corp. v. Van\$ Money Pie*, No. C98-20064 JW, 1998 U.S. Dist. LEXIS 10729, 47 U.S.P.Q.2d (BNA) 1020 (N.D. Cal. Apr. 16, 1998).

<sup>35</sup>*Trumpet Software Pty Ltd v OzEmail Pty Ltd* (1996) 34 IPR 481.

<sup>36</sup>*Specht v. Netscape Communications, Inc.*, 150 F. Supp. 2d 585 (S.D.N.Y. 2001); *Pollstar v. Gigmania Ltd.*, No. CIV-F-00-5671, 2000 U.S. Dist. LEXIS 21035 (E.D. Cal. Oct. 17, 2000).

<sup>37</sup>*Specht*, 150 F. Supp. 2d at 594–96.

## 2.4.2 Terms of licensing

As there are valid means to dictate a license agreement for computer software, some attention needs to be drawn to what the contents of license agreement can be.

### Proprietary software

Typically, software produced by large vendors is widely known as “proprietary” software. This software is licensed under terms which give the users of the software as few rights as possible. Key features of a proprietary software license (also known as an End-User License Agreement, or “EULA”) are:

- *Limitation of liability:* The vendor requires the user to waive or limit the extent to which the user holds the vendor liable for any damages caused by the software.
- *Limitation of warranty:* The vendor disclaims all warranties and guarantees which it can under law. This includes warranties such as fitness for purpose and merchantable quality which are customarily implicit in commercial transactions.
- *Limitation of activity:* The vendor restricts the use of the software to that which is necessary for the normal use of the software. Importantly, reverse engineering (except to the extent allowable by law) is invariably forbidden.
- *Limitation of modification:* The vendor restricts the ability of the user to modify the software, regardless of the purpose of any such modification.
- *Limitation of transfer:* The vendor often restricts the user from further copying the software for someone else or even from transferring the software to someone else.

- *Limitation of law or forum:* Many proprietary EULAs also include clauses as to the forum or substantive to be applied when there is a dispute about the license or the software. The forum is where someone can sue—this is typically a convenient forum for the vendor. Additionally, the substantive law which governs the license is also typically favourable to the vendor.

Some sample EULAs are [17, 46, 47, 48]. The key features noted above are present in the sample EULAs.

## **Open software**

A completely different tack to proprietary licensing can be taken—instead of keeping the code as secret, closed and proprietary as possible, it can be kept open so that users can see the source code and oftentimes modify it for their own purposes.

**Open Source** “Open source” is a term used by the Open Source Initiative to refer to software licensed under conditions which fulfil a set of criteria [49].<sup>38</sup> The Open Source Initiative believes that open source software is of better quality and more rapidly developed than proprietary equivalents. They make a business case for open source software. From their Web site, <http://www.opensource.org/>:

When programmers can read, redistribute, and modify the source code for a piece of software, the software evolves. People improve it, people adapt it, people fix bugs. And this can happen at a speed that, if one is used to the slow pace of conventional software development, seems astonishing.

We in the open source community have learned that this rapid evolutionary process produces better software than the traditional closed model, in which only a very few programmers can see the source and everybody else must blindly use an opaque block of bits.

---

<sup>38</sup>The Open Source Initiative also has a certification program [50].

Open Source Initiative exists to make this case to the commercial world.

Open Source software is licensed under conditions completely unfamiliar to typical proprietary software. The key components of the Open Source Definition are [49]:

- *Freedom of distribution*: The software must be able to be distributed without restriction. This includes being able to sell the software at a profit.
- *Availability of source code*: The source code to the software must be available. The source code must not be deliberately obfuscated, and must be the preferred form for modification of the program.
- *Freedom of derivation*: Making derived works from the software must be allowed, and the derived works must be able to be distributed under the same terms as the original software.

(An exception to this is that the author of code can insist that any derived works are labelled as such. Further, it is possible that the author can only allow modifications to be distributed as “patch files” to the original software. In this way, the origin of the software can be clearly identified for end users.)

- *No discrimination*: There must be no discrimination in the license terms against persons, groups or fields of endeavour.
- *Generality*: The license must not be dependent on the software being included in a larger distribution or part of another piece of software.

**Free software** “Free software” is a subset of open source software, premised on a more ideological basis. The Free Software Foundation, in contrast to the Open Source Initiative’s commercial pitch, focuses on the freedom of software consumers to modify their software and otherwise deal with it in a collegial and co-operative manner. The Foundation identifies four desired freedoms [32]:

0. The freedom to run the program, for any purpose;
1. The freedom to study how the program works and adapt it to specific needs;
2. The freedom to redistribute copies to help others;
3. The freedom to improve the program and release your improvements to the public for the entire community to benefit.

The freedoms are numbered from zero because the zeroth freedom is more fundamental than the others. Access to the source code for computer software is necessary for freedoms one and three. The philosophical and ideological basis for free software is essentially voluntary cooperation amongst computer users [85, 86, 87].

**Comparison with proprietary software** As a cursory comparison with the features of a proprietary license above should indicate, there is a significant difference between the permissible uses of software licensed under a proprietary license and those permitted under an open source license agreement.

The quantum shift which open source (and free software) provides has attracted the attention of some legal academics, many of whom effuse about the possible implications of the widespread use and distribution of open source software [19, 40, 45, 69].

## 2.5 Protected uses

In order to deal with the limitations customarily included in proprietary software licenses, it is necessary to protect some basic uses of computer programs. Copyright law recognises this, ensuring that some basic uses are always available to end users.

In Australia, many of these protected uses were added into the *Copyright Act* by the *Copyright Amendment (Computer Programs) Act 1999* (Cth).

An important feature of the amending Act was the introduction of section 47H, which states that any agreement or provision in agreement which attempts to exclude or limit the operation of the sections added by the Act shall have no effect. This transforms the protected uses from being a default position sure to last only as long as it takes software companies to change their boilerplate EULAs to substantive rights able to be asserted by the users of computer programs.

The Australian amendments are a tantalising step toward the United States' broad-based approach of fair use, where desired uses of computer software are protected despite the best efforts of the copyright holder.<sup>39</sup> Fair use in the United States is a defence to copyright infringement: entrenched protection for what would otherwise be copyright infringement. Although case-by-case exceptions are inherently more limited than a broader approach [26], promisingly, the exceptions in Australia cover a wide ambit of behaviours.

The Australian approach of case-by-case exception is similar to the European approach. By a 1991 Directive,<sup>40</sup> the European Council proscribed exceptions for a number of desirable uses of computer software.

### 2.5.1 Ordinary course of operation

Running a computer program involves it being copied from the secondary storage on which it resides into RAM. Being a reproduction, this is *prima facie* a copyright infringement.

In the United States, such copies were held to infringe copyright.<sup>41</sup> Copyright law was amended to overrule this decision.<sup>42</sup>

A similar process was followed in Australia. Copyright could be infringed by copying a computer program into memory,<sup>43</sup> however this is

---

<sup>39</sup>17 U.S.C. § 107.

<sup>40</sup>Directive 91/250/EC. The text of the Directive is contained in Appendix B.1.

<sup>41</sup>*MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993).

<sup>42</sup>17 U.S.C. § 117.

<sup>43</sup>*Microsoft Corp v Business Boost Pty Ltd* (2000) 49 IPR 573; [2000] FCA 1651 (17 November 2000).

now protected by statute.<sup>44</sup>

In the European Union, acts done by the lawful acquirer necessary for the use of the program are protected from infringing copyright.<sup>45</sup>

## 2.5.2 Study

Being able to study a computer program is important. Indeed, the essence of copyright protection is that it only protects the expression of an idea, not the idea itself. It should therefore be permissible to reproduce a computer program in order to study it.

In the United States, this is covered by fair use.<sup>46</sup>

In Australia, this is permitted by statute.<sup>47</sup> The studying must be done by the owner of the copyright or a licensee.<sup>48</sup> It does not apply where the copy being studied is an infringing copy.<sup>49</sup> An important restriction on the operation of the exception: the “reproduction” can not, however, be decompilation, disassembly or any other form of reverse engineering.<sup>50</sup> This reduces the ability to study a computer program except to, effectively, just use it normally.

In the European Union, this has been permitted since 1991. If someone has the right to use a computer program, they cannot be precluded from “observ[ing], study[ing] or test[ing] the functioning of the program in order to determine the ideas and principles which underlie any element of the program”.<sup>51</sup> However, like the Australian provision, a restriction on the operation of the provision is that the user can only make their observation, study or testing while performing permitted acts (which can exclude reverse engineering, except for the purpose of interoperability).

---

<sup>44</sup>*Copyright Act 1968* (Cth) s 47B(1).

<sup>45</sup>Directive 91/250/EC Article 5(1).

<sup>46</sup>17 U.S.C. § 107.

<sup>47</sup>*Copyright Act 1968* (Cth) s 47B(3).

<sup>48</sup>*Copyright Act 1968* (Cth) s 47B(3)(b).

<sup>49</sup>*Copyright Act 1968* (Cth) s 47B(4).

<sup>50</sup>*Copyright Act 1968* (Cth) s 47B(5).

<sup>51</sup>Directive 91/250/EC Article 5(3).

### 2.5.3 Back-up copies

Making a back-up copy of a computer program is also important, yet is technically forbidden by copyright law.

In the United States, it is permitted to keep a copy of a computer program for “archival purposes”, providing any archived copies are destroyed should the original copy become unlicensed.<sup>52</sup>

In Australia, making back-up copies is expressly permitted as well.<sup>53</sup> The section only applies to *bona fide* back-up copies, however: the software being backed up must have a valid license.<sup>54</sup>

In the European Union, the right of a user of a computer program to make a back-up copy is likewise protected.<sup>55</sup>

### 2.5.4 Reverse engineering

For some purposes, reverse engineering of computer software is also protected in the United States, Australia and the European Union. This is discussed in detail in Section 4.1.

## 2.6 Summary

International orthodoxy is that computer programs are protected by copyright as literary works, granting the copyright holder of a computer program the exclusive right to authorise the reproduction of the work. For computer programs, this is an extensive right because computer programs are useless unless reproduced.

Although generally software distributors reserve as many rights as possible through their license agreements, a kernel of basic uses of computer software is protected by law in the United States, Australia and the European Union.

---

<sup>52</sup>17 U.S.C. § 117.

<sup>53</sup>*Copyright Act 1968* (Cth) s 47C.

<sup>54</sup>*Copyright Act 1968* (Cth) s 47C(4), (5).

<sup>55</sup>Directive 91/250/EC Article 5(2).

# Chapter 3

## Protecting computerised data

Separately from the protection of computer programs, computerised data is also protected. In the last half-decade the protection of computerised data has been the subject of legislative consideration and promulgation. This chapter considers the protections unique to digitised data—protection separate to that provided by vanilla copyright law [25].

### 3.1 International treaties

The basis for recent legislation in the United States, Australia and the European Union is two treaties from the World Intellectual Property Organization (WIPO). As these treaties have been signed by many countries, examination of the effects of the treaty obligations is germane.

#### 3.1.1 WIPO Copyright Treaty

The WIPO Copyright Treaty (WCT), adopted in Geneva on 20 December 1996, is a re-negotiation of copyright law for a modern time (albeit influenced by the lobbying of rights holders such as record labels and movie studios).<sup>1</sup> Building upon the Berne Convention<sup>2</sup> it re-iterates the basic

---

<sup>1</sup>The text of the treaty, agreed statements and a list of parties is available at <<http://www.wipo.int/treaties/ip/copyright/index.html>>.

<sup>2</sup>Articles 1 and 3.

premise of copyright law:<sup>3</sup>

Copyright protection extends to expressions and not to ideas, procedures, methods of operation or mathematical concepts as such.

Regarding computer software, the WCT re-states the orthodox position, that computer programs are literary works:<sup>4</sup>

Computer programs are protected as literary works within the meaning of Article 2 of the Berne Convention. Such protection applies to computer programs, whatever may be the mode or form of their expression.

Building upon TRIPS, the WCT contemplates the rental of computer software.<sup>5</sup> Articles 11 and 12 contemplate the widespread digital distribution of copyrighted material. Article 11 deals with technological protection measures, providing that parties to the treaty provide legal protection to technological measures:

Contracting parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.

Article 12 communicates a similar sentiment vis-à-vis rights management information:

- (1) Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention:

---

<sup>3</sup>Article 2.

<sup>4</sup>Article 4.

<sup>5</sup>Article 7.

- (i) to remove or alter any electronic rights management information without authority;
  - (ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority.
- (2) As used in this Article, “rights management information” means 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.

The Treaty goes on to talk about enforcement of these rights, stating in Article 14:

- (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.

There are also a series of Agreed Statements to the WCT. These are essentially aids to interpretation of the treaty. Concerning Article 1(4), it was agreed that converting data into digital form is a reproduction for the purposes of copyright law:

The reproduction right, as set out in Article 9 of the Berne Convention, and the exceptions permitted thereunder, fully apply in the digital environment, in particular to the use of works in digital form. It is understood that the storage of a protected

work in digital form in an electronic medium constitutes a reproduction within the meaning of Article 9 of the Berne Convention.

Concerning Article 4, the contracting states agreed that the protection of computer programs under the WCT is consistent with other international treaties:

The scope of protection for computer programs under Article 4 of this Treaty, read with Article 2, is consistent with Article 2 of the Berne Convention and on a par with the relevant provisions of the TRIPS Agreement.

Concerning Article 12, it was agreed that rights of remuneration may also be protected by rights management schemes. Additionally, the rights management schemes should not impose additional formalities impeding the enjoyment of established rights:

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.

It is further understood that Contracting Parties will not rely on this Article to devise or implement rights management systems that would have the effect of imposing formalities which are not permitted under the Berne Convention or this Treaty, prohibiting the free movement of goods or impeding the enjoyment of rights under this Treaty.

It is primarily this treaty which has provided the basis for national legislation in the United States, Australia and the European Union.

### **3.1.2 WIPO Performance and Phonograms Treaty**

The WIPO Performances and Phonograms Treaty (WPPT) exhorts the same course of action, primarily in the context of performers.<sup>6</sup> The preamble records that the Contracting Parties:

---

<sup>6</sup>Excerpts from the WPPT are contained in Appendix A.1.

Desiring to develop and maintain the protection of the rights of performers and producers of phonograms in a manner as effective and uniform as possible,

Recognizing the need to introduce new international rules in order to provide adequate solutions to the questions raised by economic, social, cultural and technological developments,

Recognizing the profound impact of the development and convergence of information and communication technologies on the production and use of performances and phonograms,

Recognizing the need to maintain a balance between the rights of performers and producers of phonograms and the larger public interest, particularly education, research and access to information,

Have agreed ...

Performers, the focus of the WPPT, are defined as<sup>7</sup>

actors, singers, musicians, dancers, and other persons who act, sing, deliver, declaim, play in, interpret, or otherwise perform literary or artistic works or expressions of folklore.

As the preamble notes, the WPPT recognises that technology is increasingly used as a means of communicating music. To wit, it contains substantively identical provisions as the WCT for obligations concerning technological measures<sup>8</sup> and obligations concerning rights management information.<sup>9</sup> Indeed, even the Agreed Statements at the Diplomatic Conference echo each other:

The agreed statement concerning Article 12 (on Obligations concerning Rights Management Information) of the WIPO Copyright Treaty is applicable *mutatis mutandis* also to Article 19 (on Obligations concerning Rights Management Information) of the WIPO Performances and Phonograms Treaty.

The WIPO Performances and Phonograms Treaty, therefore, provides additional support in international law for nations to enact laws concerning technological protection measures of copyrighted works and rights

---

<sup>7</sup>Article 2(d).

<sup>8</sup>Article 18.

<sup>9</sup>Article 19

management information embedded in, or associated with, copyrighted works.

## 3.2 United States

The WCT and WPPT were implemented in the United States by the Digital Millennium Copyright Act. Recently, further legislation has been proposed to extend further the reach of copyright law.

### 3.2.1 Digital Millennium Copyright Act

Passed in 1998, the Digital Millennium Copyright Act (DMCA) is, according to the preamble, “An Act . . . to implement the World Intellectual Property Organization Copyright Treaty and Performances and Phonograms Treaty”. For present purposes, the key provisions introduced to United States copyright law by the DMCA are contained in a new Chapter 12, entitled “Copyright Protection and Management Systems”.<sup>10</sup>

#### **Technological protection measures**

The primary provision of the DMCA concerns technological protection measures: measures which regulate access to copyrighted works.

**Base prohibitions** The base provision of the DMCA is a broad prohibition:<sup>11</sup>

No person shall circumvent a technological measure that effectively controls access to a work protected under this title.

An additional violation is to “manufacture, import, offer to the public, provide or otherwise traffic in any technology, product, service, device, component, or part thereof that” is primarily designed to circum-

---

<sup>10</sup>17 U.S.C. §§ 1201 et seq.

<sup>11</sup>17 U.S.C. § 1201(a)(1)(A).

vent technological protection measures,<sup>12</sup> has only a limited commercial purpose other than to circumvent technological protection measures<sup>13</sup> is marketed for the circumvention of technological protection measures.<sup>14</sup>

Interestingly, despite the cries that the DMCA means the end of fair use, the DMCA itself pays lip service to the notion of fair use:<sup>15</sup>

Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title.

However, it has been held that the circumvention provisions are a new balance struck by Congress.<sup>16</sup> Indeed, fair use has effectively vanished under the DMCA [72]. This issue is further explored in Section 5.3.3.

**Non-profit libraries, archives and educational institutions** A non-profit library, archive or educational institution can make a good faith determination as to whether acquire a “commercially exploited copyrighted work” for the sole purpose of engaging in conduct allowed by copyright law without worrying about the anti-circumvention provision.<sup>17</sup>

**Law enforcement, intelligence and other government activities** Any officer, agent or employee of the United States, a State or a political subdivision of a State, or person acting pursuant to a contract with any of those entities is, for most relevant purposes, not constrained by the DMCA.<sup>18</sup>

**Interoperability** A person can circumvent technological protection measures on a lawfully obtained copy of a computer program for the sole pur-

---

<sup>12</sup>17 U.S.C. § 1201(b)(1)(A).

<sup>13</sup>17 U.S.C. § 1201(b)(1)(B).

<sup>14</sup>17 U.S.C. § 1201(b)(1)(C).

<sup>15</sup>17 U.S.C. § 1201(c).

<sup>16</sup>*Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 304, 321–324 (S.D.N.Y. 2000).

<sup>17</sup>17 U.S.C. § 1201(d).

<sup>18</sup>17 U.S.C. § 1201(e).

pose of identifying and analysing the program to create an interoperable product, providing the information was not previously readily available.<sup>19</sup>

Importantly, the circumvention must be for the “sole purpose” of creating an interoperable program. Any public dissemination of the information is impermissible.<sup>20</sup>

**Encryption research** An important reason to attempt to circumvent electronic protection measures is to engage in encryption research. Technological protection measures can be circumvented on lawfully obtained works (including phonorecords) where necessary for security research.<sup>21</sup> The researcher must have made a good faith effort to obtain authorisation from the copyright holder first,<sup>22</sup> and the circumvention cannot otherwise be unlawful.<sup>23</sup>

In order to determine whether a person was, in fact, engaging in security research the DMCA provides three factors for a court to consider.<sup>24</sup> First, whether and if so to what extent the information was disseminated and whether the dissemination facilitates copyright infringement.<sup>25</sup> Second, the extent to which the researcher can be characterised as a researcher in the field of encryption technology.<sup>26</sup> Third, whether the copyright holder is provided with notice of the findings of the research and the timeliness of such notice.<sup>27</sup> These constraints are intended to limit the availability of the exception to academics and established researchers in the field.

**To protect personally-identifying information** In accordance with the *laissez-faire* approach of the United States to privacy on the Internet, any

---

<sup>19</sup>17 U.S.C. § 1201(f)(1).

<sup>20</sup>17 U.S.C. § 1201(f)(3); see *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 320 (S.D.N.Y. 2000) (citing the legislative history).

<sup>21</sup>17 U.S.C. § 1201(g).

<sup>22</sup>17 U.S.C. § 1201(g)(2)(C).

<sup>23</sup>17 U.S.C. § 1201(g)(2)(D).

<sup>24</sup>17 U.S.C. § 1201(g)(3).

<sup>25</sup>17 U.S.C. § 1201(g)(3)(A).

<sup>26</sup>17 U.S.C. § 1201(g)(3)(B).

<sup>27</sup>17 U.S.C. § 1201(g)(3)(C).

circumvention of a protection measure where the information that is being protected is personally identifying information about the online activities of a natural person.<sup>28</sup> This license to circumvent is restricted: the collection of information must be surreptitious,<sup>29</sup> the circumvention must have the sole effect of identifying and disabling the information collection capability<sup>30</sup> and the circumvention is for the sole purpose of preventing the collection of the information and isn't otherwise prohibited.<sup>31</sup>

**Security testing** Technological protection measures may have security implications (they are often kept secret and proprietary [18]), therefore there is an exception for "accessing a computer, computer system, or computer network, solely 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>32</sup> as long as it does not otherwise constitute a violation of law.<sup>33</sup>

Like the encryption research provision, there are two factors to be taken into account by a court when considering whether the exception should apply.<sup>34</sup> First, whether the information resulting from the security testing is used solely to promote the security of the tested systems or networks.<sup>35</sup> Second, whether the information resulting from the security testing facilitates the infringement of privacy or other law.<sup>36</sup>

### **Copyright management information**

The DMCA provides that no person can, with the intent to induce, enable, facilitate or conceal copyright infringement, provide, distribute or import

---

<sup>28</sup>17 U.S.C. § 1201(i)(1)(A).

<sup>29</sup>17 U.S.C. § 1201(i)(1)(B).

<sup>30</sup>17 U.S.C. § 1201(i)(1)(C).

<sup>31</sup>17 U.S.C. § 1201(i)(1)(D).

<sup>32</sup>17 U.S.C. § 1201(j)(1).

<sup>33</sup>17 U.S.C. § 1201(j)(2).

<sup>34</sup>17 U.S.C. § 1201(j)(3).

<sup>35</sup>17 U.S.C. § 1201(j)(3)(A).

<sup>36</sup>17 U.S.C. § 1201(j)(3)(B).

false copyright management information.<sup>37</sup>

Further, no person can without the consent of the copyright owner or legal authority<sup>38</sup>

- (1) intentionally remove or alter any copyright management information,
- (2) distribute or import for distribution copyright management information knowing that the copyright management information has been removed or altered without authority of the copyright owner or the law, or
- (3) distribute, import for distribution, or publicly perform works, copies of works, or phonorecords, knowing that copyright management information has been removed or altered without authority of the copyright owner or the law,

if they know it will induce, enable, facilitate or conceal copyright infringement. For civil actions, it is merely sufficient that the person had reason to know. There is also no liability for law enforcement or governmental agents.<sup>39</sup>

### **Civil remedies**

“Any person injured” by a breach of one of the above sections can bring action in an appropriate United States District Court.<sup>40</sup> In such an action, the court can grant injunctions,<sup>41</sup> can impound<sup>42</sup> and subsequently order the destruction of devices,<sup>43</sup> award the recovery of costs<sup>44</sup> and attorney’s fees.<sup>45</sup>

---

<sup>37</sup>17 U.S.C. § 1202(a).

<sup>38</sup>17 U.S.C. § 1202(b)

<sup>39</sup>17 U.S.C. § 1202(d). This provision is substantively identical to 17 U.S.C. § 1201(e).

<sup>40</sup>17 U.S.C. § 1203(a).

<sup>41</sup>17 U.S.C. § 1203(b)(1).

<sup>42</sup>17 U.S.C. § 1203(b)(2).

<sup>43</sup>17 U.S.C. § 1203(b)(6).

<sup>44</sup>17 U.S.C. § 1203(b)(4).

<sup>45</sup>17 U.S.C. § 1203(b)(5).

The court can also award damages.<sup>46</sup> The damages can consist of either actual damages (those suffered by the party bringing the action and the profits of the violator attributable to a violation) or statutory damages (a prescribed sum per violation).<sup>47</sup> The court can award triple damages for repeated violations,<sup>48</sup> and reduce the amount of damages for violation where the violator was not aware and had no reason to be aware they were violating the law.<sup>49</sup>

### **Criminal remedies**

Any person (excepting a non-profit library, archive or educational institution<sup>50</sup>) who violates sections 1201 or 1202 “willfully and for purposes of commercial advantage or private financial gain” is also liable for criminal penalties.<sup>51</sup> The first offence is punishable by \$500,000 and five years imprisonment.<sup>52</sup> Subsequent offences attract a doubled maximum penalty.<sup>53</sup>

### **Intermediate copies during transit**

Recognising that intermediate copies are often made during the transfer of files over the Internet, the DMCA addresses the issue of intermediate liability.<sup>54</sup> “However, the DMCA’s cumbersome and disorganized structure makes its provisions difficult to untangle” [101]. The DMCA recognises and protects:

- *Transitory network communications*: Reproductions of copyrighted material made by a passive network provider who, without manual intervention, provides connectivity;<sup>55</sup>

---

<sup>46</sup>17 U.S.C. § 1203(b)(3), (c).

<sup>47</sup>17 U.S.C. § 1203(c)(2)–(3).

<sup>48</sup>17 U.S.C. § 1203(c)(4)

<sup>49</sup>17 U.S.C. § 1203(c)(5).

<sup>50</sup>17 U.S.C. § 1204(b).

<sup>51</sup>17 U.S.C. § 1204(a).

<sup>52</sup>17 U.S.C. § 1204(a)(1).

<sup>53</sup>17 U.S.C. § 1204(a)(2).

<sup>54</sup>17 U.S.C. § 512

<sup>55</sup>17 U.S.C. § 512(a).

- *System caching*: Network providers who provide caches of information (in accordance with relevant technological standards) to provide better network efficiency are protected against copyright infringement actions for the contents of their caches,<sup>56</sup>
- *Safe harbour*: Operators of networks containing user data are not liable for infringing content on the networks if the network operators (a) do not have actual knowledge of the infringement, (b) is not aware of facts or circumstances from which it would be apparent that infringement is taking place, or (c) upon learning of the infringement expeditiously acts to remove or disable access to the infringing material;<sup>57</sup>
- *Search engines*: Reproductions of copyrighted material made in order to facilitate linking or indexing of material are protected from copyright infringement.<sup>58</sup>

These protections do not apply to the circumvention provisions—they are not available where an action has been brought alleging trafficking in a circumvention device.<sup>59</sup>

### 3.2.2 Recent legislative proposals

The Security Systems Standards and Certification Act (SSSCA) is U.S. legislation proposed by Senator Fritz Hollings, chairman of the Senate Commerce Committee [68]. A working draft of the proposed legislation is available [84]. Essentially, it seeks to ensure all digital devices contain federally-mandated copy protection technology;<sup>60</sup> to produce a device without such facilities would be illegal and to remove or alter the security technology would likewise attract sanction.<sup>61</sup>

---

<sup>56</sup>17 U.S.C. § 512(b).

<sup>57</sup>17 U.S.C. § 512(c).

<sup>58</sup>17 U.S.C. § 512(d).

<sup>59</sup>*Universal City Studios, Inc. v. Reimerdes*, 82 F. Supp. 2d 211, 217 (S.D.N.Y. 2000).

<sup>60</sup>SSSCA § 101.

<sup>61</sup>SSSCA § 103(a).

The only defence available to infractions is the time-shifting network television.<sup>62</sup> This exception is, however, exceedingly narrow and is essentially limited to the facts of *Sony Corp. v. Universal City Studios, Inc.*<sup>63</sup>

Reaction to this legislation has largely been by way of condemnation; this is discussed in Section 5.3.5.

### 3.3 Australia

Soon after the United States Congress passed the Digital Millennium Copyright Act, the Australian Parliament proposed similar reforms. These reforms were known as the Digital Agenda reforms, and were implemented by the *Copyright Amendment (Digital Agenda) Act 2000* (Cth).

#### 3.3.1 Copyright Amendment (Digital Agenda) Act

The *Copyright Amendment (Digital Agenda) Act 2000* (Cth) is largely complementary legislation to the *Copyright Amendment (Computer Programs) Act 1999* (Cth). Indeed, many of the amendments are minor wording changes to provisions introduced by the *Copyright Amendment (Computer Programs) Act*. For this thesis, the most important provisions of the Act are the circumvention provisions, contained in a new Division 2A (entitled "Actions in relation to circumvention devices and electronic rights management information") to Part V ("Remedies and offences").

#### Circumvention devices

Section 116A regulates circumvention devices and circumvention services.

**Definitions** A circumvention device is, essentially, a device which is designed to circumvent a technological protection measure:<sup>64</sup>

---

<sup>62</sup>SSSCA § 103(b).

<sup>63</sup>*Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984). The case is examined in more detail in Section 5.3.1.

<sup>64</sup>*Copyright Act 1968* (Cth) s 10(1).

a device (including a computer program) having only a limited commercially significant purpose or use, or no such purpose or use, other than the circumvention, or facilitating the circumvention, of an effective technological protection measure.

A circumvention service is a service having the same effect as a circumvention device.<sup>65</sup> A technological protection measure is a means of regulating access to a work so as to prevent copyright infringement.<sup>66</sup>

a device or product, or a component incorporated into a process, that is designed, in the ordinary course of its operation, to prevent or inhibit the infringement of copyright in a work or other subject-matter by either or both of the following means:

- (a) by ensuring that access to the work or other subject matter is available solely by use of an access code or process (including decryption, unscrambling or other transformation of the work or other subject-matter) with the authority of the owner or licensee of the copyright;
- (b) through a copy control mechanism.

**Prohibition** If data<sup>67</sup> is protected by a technological protection measure, then a person can't without the consent of the copyright owner of the data deal with that circumvention device. The section applies to a person who:<sup>68</sup>

- (i) makes a circumvention device capable of circumventing, or facilitating the circumvention of, the technological protection measure;
- (ii) sells, lets for hire, or by way of trade offers or exposes for sale or hire or otherwise promotes, advertises or markets, such a circumvention device;

---

<sup>65</sup>*Copyright Act 1968* (Cth) s 10(1).

<sup>66</sup>*Copyright Act 1968* (Cth) s 10(1).

<sup>67</sup>The data itself must be capable of copyright protection, being either a "work" or "subject-matter" within the meaning of the *Copyright Act*.

<sup>68</sup>*Copyright Act 1968* (Cth) s 116A(1)(b).

- (iii) distributes such a circumvention device for the purpose of trade, or for any other purpose that will affect prejudicially the owner of the copyright;
- (iv) exhibits such a circumvention device in public by way of trade;
- (v) imports such a circumvention device into Australia for the purpose of:
  - (A) selling, letting for hire, or by way of trade offering or exposing for sale or hire or otherwise promoting, advertising or marketing, the device; or
  - (B) distributing the device for the purpose of trade, or for any other purpose that will affect prejudicially the owner of the copyright; or
  - (C) exhibiting the device in public by way of trade;
- (vi) makes such a circumvention device available online to an extent that will affect prejudicially the owner of the copyright;
- (vii) provides, or by way of trade promotes, advertises or markets, a circumvention service capable of circumventing, or facilitating the circumvention of, the technological protection measure

The person must have known, or ought reasonably have known, that the device or service would facilitate circumvention,<sup>69</sup> although the defendant must disprove the presumption that he or she knew.<sup>70</sup> Additionally, the prohibition does not apply in relation to anything lawfully done for the purposes of law enforcement or national security or on behalf of a federal, State or Territory government or governmental authority.<sup>71</sup>

**Exceptions** There are also exceptions where the use will be for a “permitted purpose”. A “permitted purpose” is, essentially, a purpose which is permitted under the *Copyright Act*:<sup>72</sup> reproducing for interoperability,<sup>73</sup> re-

<sup>69</sup> *Copyright Act 1968* (Cth) s 116A(1)(c).

<sup>70</sup> *Copyright Act 1968* (Cth) s 116A(6).

<sup>71</sup> *Copyright Act 1968* (Cth) s 116A(2).

<sup>72</sup> *Copyright Act 1968* (Cth) s 116A(3)(b)(iv).

<sup>73</sup> *Copyright Act 1968* (Cth) s 47D.

producing for error correction,<sup>74</sup> reproducing for security testing,<sup>75</sup> copying by the Parliamentary library for members of Parliament,<sup>76</sup> reproducing and communicating by libraries and archives for users<sup>77</sup> or other libraries,<sup>78</sup> reproducing and communicating for preservation,<sup>79</sup> use for the Crown<sup>80</sup> or by educational institutions.<sup>81</sup> Fair dealing is not included (see Section 5.3.3). Additionally, it is not an exception to circumvent a technological protection measure as part of the study of a computer program, further undercutting the utility of section 47B.

For the making or importation of a device or service, the device must be for use only with data that is not readily available in a non-technologically protected form<sup>82</sup> or to supply the device or service for use only for a permitted purpose.<sup>83</sup>

It also does not apply where the device or service is supplied to a person (who can legally perform the reproductions for a permitted purpose<sup>84</sup>) who gives the supplier a signed declaration essentially saying that they'll only use it for a permitted purpose.<sup>85</sup>

Also, unlike the DMCA, there is no prohibition on the use of a circumvention device. However, in order to use a circumvention device, one must first obtain it. The *Digital Agenda* reforms focus on the obverse side of use. This focuses enforcement effort on the larger entities (consumers are usually individuals) and removes the spectre of liability from consumers—if one has a circumvention device then section 116A does not apply (providing it isn't self-built and you don't intend to further distribute it).

---

<sup>74</sup>Copyright Act 1968 (Cth) s 47E.

<sup>75</sup>Copyright Act 1968 (Cth) s 47F.

<sup>76</sup>Copyright Act 1968 (Cth) s 48A.

<sup>77</sup>Copyright Act 1968 (Cth) s 49.

<sup>78</sup>Copyright Act 1968 (Cth) s 50.

<sup>79</sup>Copyright Act 1968 (Cth) s 51A.

<sup>80</sup>Copyright Act 1968 (Cth) s 183.

<sup>81</sup>Copyright Act 1968 (Cth) Part VB.

<sup>82</sup>Copyright Act 1968 (Cth) s 116A(4)(a).

<sup>83</sup>Copyright Act 1968 (Cth) s 116A(4)(b).

<sup>84</sup>Copyright Act 1968 (Cth) s 116A(8).

<sup>85</sup>Copyright Act 1968 (Cth) s 116A(3).

## Rights management information

Like the WCT which it implements and the DMCA which it succeeds, the *Digital Agenda* amendments also deal with rights management information. Any person who removes or alters electronic rights management information on a work in which copyright subsists<sup>86</sup> is without the permission of the copyright owner<sup>87</sup> is liable to suit to the copyright owner or exclusive licensee.<sup>88</sup>

As with the circumvention device provisions, the person doing the removing must know, or ought reasonably to have known, the removal of the information would “induce, enable, facilitate or conceal” a copyright infringement.<sup>89</sup> The burden of disproving this falls on the defendant.<sup>90</sup>

A supplementary provision, section 116C, regulates commercial dealings with works whose electronic rights management information has been tampered with. If (without the consent of the copyright owner or exclusive licensee<sup>91</sup>) a person distributes for trade purposes, imports for trade purposes or communicates to the public data that has removed or altered rights management information<sup>92</sup> is subject to action by the copyright owner or exclusive licensee.<sup>93</sup>

The person must know the data had the rights management information removed or altered without authorization<sup>94</sup> and knew, or ought reasonably to have known, that the removal or alteration would “induce, enable, facilitate or conceal” an infringement of the copyright.<sup>95</sup> The burden of disproving the knowledge is on the defendant, like the above provisions.<sup>96</sup>

---

<sup>86</sup> *Copyright Act 1968* (Cth) s 116B(1)(a)

<sup>87</sup> *Copyright Act 1968* (Cth) s 116B(1)(b)

<sup>88</sup> *Copyright Act 1968* (Cth) s 116B(2).

<sup>89</sup> *Copyright Act 1968* (Cth) s 116B(1)(c).

<sup>90</sup> *Copyright Act 1968* (Cth) s 116B(3).

<sup>91</sup> *Copyright Act 1968* (Cth) s 116C(1)(a).

<sup>92</sup> *Copyright Act 1968* (Cth) s 116C(1)(b).

<sup>93</sup> *Copyright Act 1968* (Cth) s 116C(2).

<sup>94</sup> *Copyright Act 1968* (Cth) s 116C(1)(c).

<sup>95</sup> *Copyright Act 1968* (Cth) s 116C(1)(d).

<sup>96</sup> *Copyright Act 1968* (Cth) s 116C(3).

## Remedies

If an action under section 116A, 116B or 116C is proved, a court may order an injunction and either damages or an account of profits.<sup>97</sup> The court may also order additional damages based on any relevant factors, including the flagrancy of the defendant's actions and any benefit shown to the defendant.<sup>98</sup>

These are standard provisions and the additional damages discretion provides the court with tools to protect copyright owners from flagrant violators.

## Criminal sanctions

In Australia, copyright violation can be a criminal offence, especially where the violation is especially egregious.<sup>99</sup> The circumvention device and rights management provisions also have criminal analogues.<sup>100</sup>

In substance, they are essentially the same as the civil liability provisions (discussed above) but the state of mind of the defendant is different. Instead of merely knowing, or having reason to know, the illicit use of the device or data, the defendant must know or be reckless as to whether the illicit use can be facilitated.<sup>101</sup> The same defences and limitations as for the civil liability provisions apply.<sup>102</sup>

Any person who violates those provisions is liable for imprisonment of up to five years or a fine of up to \$60,500.<sup>103</sup> A corporation is liable to a fine five times greater.<sup>104</sup>

---

<sup>97</sup>*Copyright Act 1968* (Cth) s 116D(1).

<sup>98</sup>*Copyright Act 1968* (Cth) s 116D(2).

<sup>99</sup>*Copyright Act 1968* (Cth) s 132.

<sup>100</sup>*Copyright Act 1968* (Cth) s 132(5A)–(5J).

<sup>101</sup>*Copyright Act 1968* (Cth) s 132(5A), (5B), (5C), (5D)(e).

<sup>102</sup>*Copyright Act 1968* (Cth) s 132(5E), (5F), (5G).

<sup>103</sup>*Copyright Act 1968* (Cth) s 132(6A) provides that a breach of s 132(5A) is punishable by a fine of not more than 550 penalty units. A penalty unit is \$110: *Crimes Act 1914* (Cth) s 4AA.

<sup>104</sup>*Crimes Act 1914* (Cth) s 4B(3).

### Intermediate copying during transmission

In Australia, one of the amendments introduced in the *Copyright Amendment (Digital Agenda) Act 2000* (Cth) dealt with this issue. Section 43A of the *Copyright Act 1968* (Cth) provides that any reproduction of software “as part of the technical process of making or receiving a communication” is not an infringement of copyright.<sup>105</sup> The effect of this provision is discussed in Section 5.3.4.

## 3.4 The European Union

The European Union has also taken steps to implement the WCT provisions. Despite work beginning soon after the passing of the treaty in 1996, the European Union Council has only recently (April 9, 2001) accepted a directive designed to comply with the requirements [22]. For the most part, the provisions are substantively similar to analogous provisions in the DMCA and the *Copyright Amendment (Digital Agenda) Act* and, as such, will only be briefly described here. Relevant provisions from the Directive are extracted in Appendix B.2.

In broad general terms, Article 5 provides for the indemnity of network access providers for the mechanical reproduction of online material.

The protections of Article 6 of the Directive are of a similar scope to that provided for by the United States’ Digital Millennium Copyright Act and Australia’s *Copyright Amendment (Digital Agenda) Act*.<sup>106</sup> The exceptions which are provided are minimal. It also suffers from the same basic problem: it veils technological measures with legal protection even if the technological measures protect rights which are not granted to the copyright holder.

Article 7 provides similar protection for rights management information. Additionally, Article 12 provides that “[n]ot later than 22 December 2004, and every three years thereafter”, a report on the effect of, *inter alia*,

---

<sup>105</sup>*Copyright Act 1968* (Cth) s 43A(1).

<sup>106</sup>The text of Article 6 is in Appendix B.2.

Article 6 (but not Article 7) will be submitted by the Commission to the European Parliament.

### 3.5 The United Kingdom

The United Kingdom is, of course, part of the European Union. However, the *Copyright, Patents and Designs Act 1988* (UK) has a long-standing prohibition against the circumvention of copy-protection technology. Section 296 (with the marginal note of “Devices designed to circumvent copy-protection”) provides, relevantly:

- (1) This section applies where copies of a copyright work are issued to the public, by or with the licence of the copyright owner, in an electronic form which is copy-protected.
- (2) 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.
- ...
- (4) References in this section to copy-protection include any device or means intended to prevent or restrict copying of a work or to impair the quality of copies made.
- (5) Expressions used in this section which are defined for the purposes of Part I of this Act (copyright) have the same meaning as in that Part.

...

For legislative drafting approximately ten years ahead of its time, there are significant similarities with the WCT provisions. Although the term

“copy-protection” is not defined in the Act, it is clearly an analogous concept to the technological protection measures contemplated by the WCT, DMCA and Digital Agenda reforms.

### **3.6 Summary**

Because domestic legislative reform for the copyright protection of computerised data came from a common base, namely the WCT, the protection in the United States, Australia and the European Union is substantially uniform. The United Kingdom legislation, although written and passed a decade before the WCT, echoes the later instrument’s language.

## Chapter 4

# Applying the law to the technology

The heretofore latent tension between copyright and technology has recently been made apparant in several distinct factual scenarios. The facts and technology behind some of these scenarios will be examined in this chapter, as well as the legal implications.

### 4.1 Reverse engineering

Generally speaking, reverse engineering is a permitted use of copyrighted works. You can reverse engineer something to see how it works, then do the same thing in a different way. This is the essence of copyright protection—it only protects the expression of a work, not the general ideas which underlie it.

Computer software is, however, different. In order to examine how a computer program works, it needs to be reproduced. Therefore, a copyright holder in a computer program could—theoretically—preclude any reverse engineering as part of the license agreement, as reproduction is an exclusive right granted to the copyright holder.

This would seem to be manifestly unfair. If the purpose of the reverse engineering is not to copy code but merely to re-implement concepts, then to prohibit reverse engineering would be to permit patent-like protection

for the bargain-basement price of copyright [1]. This would seem to be contrary to public policy, as well as the original stated goals of copyright protection.

### 4.1.1 European Union

The European Union was the first jurisdiction to acknowledge the utility of reverse engineering for the purpose of interoperability. With Directive 91/250/EEC, passed on 14 May 1991, expressly permitted the reverse engineering of computer programs “to achieve the interoperability of an independently created computer program with other programs”.<sup>1</sup> The full text of the directive is contained in Appendix B.1.

There are conditions on this largess. The program being reverse engineered must be a valid licensed copy,<sup>2</sup> the information required for creating an interoperable product must not be readily available,<sup>3</sup> the reverse engineering is limited to the extent necessary to achieve interoperability,<sup>4</sup> the information must not be used for any other purpose than to develop the interoperable product,<sup>5</sup> and unnecessary further dissemination is prohibited.<sup>6</sup>

The Directive also provides that reproduction is permissible, regardless of the license on the software, for the purposes of error correction,<sup>7</sup> or studying the program in order to determine the underlying principles of its operation.<sup>8</sup>

### 4.1.2 United States

In the United States, the epicentre of the computing revolution, this matter arose in litigation in the early 1990s. The United States Court of Appeals,

---

<sup>1</sup>Article 6.

<sup>2</sup>Article 6(1)(a).

<sup>3</sup>Article 6(1)(b).

<sup>4</sup>Article 6(1)(c).

<sup>5</sup>Article 6(2)(a).

<sup>6</sup>Article 6(2)(b).

<sup>7</sup>Article 5(1).

<sup>8</sup>Article 5(3).

the federal court immediately below the Supreme Court, used the “fair use” defence to copyright infringement to allow reverse engineering for interoperability.

### **Fair use emerges**

In *Sega Enterprises Ltd. v. Accolade, Inc.*,<sup>9</sup> Sega, a games console maker, sued Accolade, a game manufacturer, because Accolade did not license information about the Sega Genesis console from Sega. Instead, Accolade reverse engineered Sega’s video game programs and looked closely at a Genesis console when the games were loaded. Accolade then produced a game development manual that was followed by its game developers.

Sega sued for copyright infringement as Accolade had made unauthorised reproductions of Sega’s computer programs. Accolade argued that their reproductions were a fair use of Sega’s work. Fair use is a defence to copyright infringement in the United States.<sup>10</sup> In deciding whether the fair use defence is established, the court must look at four factors:

1. the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
2. the nature of the copyrighted work;
3. the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
4. the effect of the use upon the potential market for or value of the copyrighted work.

The Court of Appeals for the Ninth Circuit first noted that Accolade’s commercial use tended against a finding of fair use.<sup>11</sup> However, despite the fact that Accolade was a commercial manufacturer of games cartridges, the information about the Sega internals was only incidental to the

---

<sup>9</sup>977 F.2d 1510 (9th Cir. 1992), amended at 1993 U.S. App. LEXIS 78 (9th Cir. Jan. 6, 1993)

<sup>10</sup>17 U.S.C. § 107.

<sup>11</sup>977 F.2d at 1522 (citing *Harper & Row Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539, 562 (1985)).

commercial use of Accolade—the originality of the games which Accolade was producing was not in issue.<sup>12</sup>

Second, with respect to the fourth factor, the court engaged in a similar analysis. Accolade, the court found, intended to become a legitimate competitor to Sega in the video games market. Within that market, it is the quality of the games which is the primary differentiation, not the information which Accolade had reverse engineered.<sup>13</sup>

Third, considering the second statutory factor, the court noted the dilemma of the Court of Appeals for the Second Circuit in *Computer Associates International, Inc. v. Altai, Inc.*,<sup>14</sup> and accepted that not all aspects of computer programs are entitled to complete protection. The court accepted that Accolade’s reverse engineering was primarily an identification of the functional aspects of the Sega system.<sup>15</sup>

The final statutory factor, the third, weighed against Accolade. Accolade reverse engineered Sega programs. However, this alone does not prevent a finding of fair use, and the factor is given little weight where the ultimate use of the work is minimal, as was the case with Accolade.<sup>16</sup>

Therefore, the court rejected Sega’s copyright-based claims, stating:<sup>17</sup>

[W]here disassembly is the only way to gain access to the ideas and functional elements embodied in a copyrighted computer program and where there is a legitimate reason for seeking such access, disassembly is a fair use of the copyrighted work, as a matter of law.

This decision was consistent with a then-recent decision of the Court of Appeals for the Federal Circuit,<sup>18</sup> and has recently been applied by the Court of Appeals for the Ninth Circuit.<sup>19</sup>

---

<sup>12</sup>977 F.2d at 1522–23.

<sup>13</sup>977 F.2d at 1523–24.

<sup>14</sup>23 U.S.P.Q.2d (BNA) 1241 (2d Cir. 1992).

<sup>15</sup>977 F.2d at 1524–26.

<sup>16</sup>977 F.2d at 1526–27.

<sup>17</sup>977 F.2d at 1527–28.

<sup>18</sup>*Atari Games Corp. v. Nintendo of America, Inc.*, 975 F.2d 832 (Fed. Cir. 1992).

<sup>19</sup>*Sony Computer Entertainment, Inc. v. Connectix Corp.* 203 F.3d 596 (9th Cir. 2000), cert. denied, 531 U.S. 871 (2000).

### **An alternate analysis: copyright misuse?**

It has been suggested by some academics that fair use was not the most appropriate doctrine to use in this situation. The plaintiffs in the cases were seeking to protect ideas with copyright—a behaviour which smacks of misuse as the copyright holders attempted to protect more than just the particular expression of an idea.

Patent misuse has long been established as a defence to an action of patent infringement, applied by courts on the basis of anti-trust principles.<sup>20</sup> Copyright misuse is a doctrine which is known to United States law, although it has not been eagerly embraced by courts. The Supreme Court of the United States, by dicta, approved the notion of copyright misuse.<sup>21</sup> In recent years, Courts of Appeal have also accepted that copyright misuse may apply.<sup>22</sup>

A copyright misuse defence, it is argued [36, 38], can provide more satisfactory protection in the context of computer software. It focuses on the conduct of the copyright owner, not the use of the alleged copyright violator. As such, it is doctrinally more appropriate for many reverse engineering cases.

As copyright misuse has not found judicial support, the theory is largely a matter of academic interest.

### **4.1.3 Australia**

Reverse engineering also occurred, and was litigated in Australia. Unlike the United States, Australian law did not permit reverse engineering without explicit legislative intervention.

---

<sup>20</sup>See 35 U.S.C. § 271(d)(5).

<sup>21</sup>*Morton Salt Co. v. G. S. Suppiger Co.*, 314 U.S. 488, 494 (1942) (citing *Edward Thompson Co. v. American Law Book Co.*, 122 F. 922, 966 (2d Cir. 1903); *Stone & M'Carrick v. Dugan Piano Co.*, 220 F. 837, 841–43 (5th Cir. 1915)).

<sup>22</sup>*Alcatel USA, Inc. v. DGI Technologies, Inc.*, 166 F.3d 772 (5th Cir. 1999); *Practice Management Information Corp. v. American Medical Assn'n*, 121 F.3d 516 (9th Cir. 1996); *Lasercomb America, Inc. v. Reynolds*, 911 F.2d 970 (4th Cir. 1990).

### *Autodesk Inc v Dyason*

The first litigation on this point was the *Autodesk v Dyason* saga. The basic facts of the case were that Autodesk produced software called AutoCAD. In order to discourage piracy of AutoCAD, it required a “dongle” in order to run. This dongle plugged into the serial port of the user’s machine, and was supplied with every valid license of AutoCAD. A part of the AutoCAD program, “Widget C”, periodically sent challenges to the serial port, and if the expected response was not forthcoming, the AutoCAD program would not continue to run.

The Dyasons decided to produce a product similar to the AutoCAD dongle. They reverse engineered the AutoCAD dongle, by means of an oscilloscope and other such technology. The product of their efforts was a replacement for the AutoCAD dongle, which they called an “Auto Key Lock”. Whereas the AutoCAD lock used a shift register to encode the challenge-response codes, the Auto Key Lock used an EPROM. The two devices were clearly different in implementation, but not in function.

Autodesk sued the Dyasons for copyright infringement. Autodesk argued that the behaviour of the dongle constituted a computer program, and the Auto Key Lock was an unauthorised reproduction of it. The matter was ultimately appealed to the High Court of Australia.<sup>23</sup>

In the High Court,<sup>24</sup> the leading judgment was written by Justice Dawson. His Honour held that the look-up table of Widget C had been reproduced by the Auto Key Lock. Although the look-up table was not itself a computer program, it was still a “substantial, indeed essential part” of the computer program comprised in Widget C.

After the decision, an application was made to re-argue the case, focusing on two new grounds:<sup>25</sup>

1. the look-up table in Widget C did not amount to a set of instructions

---

<sup>23</sup>The decision of Justice Northrop at first instance is *Autodesk Inc v Dyason* (1989) 15 IPR 1; the appeal to the Full Court of the Federal Court is *Dyason v Autodesk Inc* (1990) 24 FCR 147; 96 ALR 57; 18 IPR 109.

<sup>24</sup>*Autodesk Inc v Dyason* (1992) 173 CLR 330; 104 ALR 563; 22 IPR 163.

<sup>25</sup>*Autodesk Inc v Dyason (No 2)* (1993) 176 CLR 300; 111 ALR 385; 25 IPR 33.

but was simply data; and

2. the look-up table was not a substantial part of the Widget C program

The High Court by majority dismissed the application as, their Honours reasoned, there was ample opportunity to raise the issues during the first appearance before the High Court.

This had the effect of leaving *Autodesk v Dyason* as the governing law on copyright infringement in Australia. The High Court's decision showed "a tendency to protect the idea rather than the expression of the idea (despite a 'ritual incantation' of basic copyright principles)" [70].

Decisions of the Federal Court in subsequent years mitigated the harshness of this approach.<sup>26</sup> This mitigation was validated by the recent High Court decision in *Data Access Corporation v Powerflex Services Pty Ltd*.

### ***Data Access Corporation v Powerflex Services Pty Ltd***

The Powerflex litigation<sup>27</sup> was also based on reverse engineering. Data Access Corporation was an American company which produced and marketed a database product called Dataflex. Dr. Bennett was a medical practitioner who thought that he could do a better job. So, over a period of a couple of years, he slept less at night and gave up any leisure activities to produce a similar (and largely interoperable) product to Dataflex, which he called Powerflex (later renamed to PFXplus).

Data Access sued Dr. Bennett and his company, Powerflex Services Pty Ltd, for copyright infringement.<sup>28</sup> Before the High Court of Australia, Data Access argued three separate claims of infringement by PFXplus:<sup>29</sup>

1. The reserved words in the Dataflex system (see Section 2.3.2);

---

<sup>26</sup>*Coogi Australia Pty Ltd v Hysport International Pty Ltd* (1998) 86 FCR 154; 157 ALR 247; 41 IPR 593; *Admar Computer Pty Ltd v Ezy Systems Pty Ltd* (1997) 38 IPR 659.

<sup>27</sup>Culminating in *Data Access Corporation v Powerflex Services Pty Ltd* (1999) 202 CLR 1; 166 ALR 228; 45 IPR 353; [1999] HCA 49 (30 September 1999).

<sup>28</sup>*Data Access Corporation v Powerflex Services Pty Ltd* (1996) 33 IPR 194. Powerflex appealed this decision to the Full Court of the Federal Court: *Powerflex Services Pty Ltd v Data Access Corporation* (1997) 137 ALR 498; 37 IPR 436.

<sup>29</sup>[1999] HCA 49 at 16.

2. The macros in the Dataflex system;
3. The Huffman compression table for compressing Dataflex files.

**The macros** As well as reserved words in the Dataflex language, there were also a set of macros: commands in the Dataflex language performing a more complex function than any of the reserved words.<sup>30</sup> The evidence was clear that although Dr. Bennett replicated the functionality of the macros, it was done by careful examination of the Dataflex program, not by any process of translating the source code from one language to another but by writing original code to perform the same functionality.<sup>31</sup>

As there was no translation of the Dataflex source code, the PFXplus source code could not be an adaptation of the Dataflex code for the purposes of the *Copyright Act*. Accordingly, there was no infringement.<sup>32</sup>

**The Huffman compression table** One feature of Dataflex was a feature to save data files in a compressed form. The implementation of this compression was with a Huffman compression table. The same table was used for all compressed files.<sup>33</sup>

Standard files are represented by computers using a fixed number of bits for each character. For the 127 characters in standard ASCII, seven bits are necessary for each character to have a unique encoding. Codes such as ASCII are easy for programs to process, but are wasteful of memory. Huffman compression provides a way to reduce the file size.

Rather than using a fixed bit length encoding for each character, Huffman compression uses a variable bit length encoding. Characters are generally encoded such that the most frequently occurring characters are assigned the smallest encodings, and less frequently occurring characters are assigned larger encodings.<sup>34</sup> It has been noted that [16]:

---

<sup>30</sup>[1999] HCA 49 at 99.

<sup>31</sup>[1999] HCA 49 at 106–07.

<sup>32</sup>[1999] HCA 49 at 111.

<sup>33</sup>[1999] HCA 49 at 113–16.

<sup>34</sup>[1999] HCA 49 at 113–15.

Huffman codes are a widely used and very effective technique for compressing data; savings of 20% to 90% are typical, depending on the characteristics of the file being compressed.

Since Dataflex only used one Huffman encoding table, Dr. Bennett only needed to discern this table. To do so, Dr. Bennett did not reverse engineer the program. Instead, he used carefully constructed data files, which he saved with the compression option turned on. After examining the compressed files, he discerned the Huffman encoding of all possible characters with the Dataflex table.<sup>35</sup> The High Court upheld Data Access's arguments that this was a breach of copyright.<sup>36</sup> Data Access held copyright in the table as a separate literary work (tables and compilations are included in the statutory definition).<sup>37</sup> Dr. Bennett reproduced this table. The method used to copy the table was immaterial, and a copyright violation was found to subsist.

The reproduction of the Huffman table was solely to enable interoperability of Dataflex and PFXplus. It was a convenience to users who often used compression when saving their Dataflex files, and wanted to read them using PFXplus. The High Court recognised this, but deferred the matter to the legislature:<sup>38</sup>

The finding that the respondents infringed the appellant's copyright in the Huffman table embedded in the Dataflex program may well have considerable practical consequences. Not only may the finding affect the relations between the parties to these proceedings, it may also have wider ramifications for anyone who seeks to produce a computer program that is compatible with a program produced by others. These are, however, matters that can be resolved only by the legislature reconsidering and, if it thinks it necessary or desirable, rewriting the whole of the provisions that deal with copyright in computer programs.

Federal Parliament had already considered the issue by the time the

---

<sup>35</sup>[1999] HCA 49 at 117–18.

<sup>36</sup>[1999] HCA 49 at 124.

<sup>37</sup>[1999] HCA 49 at 121–22.

<sup>38</sup>[1999] HCA 49 at 125.

High Court delivered its decision on 30 September 1999. The *Copyright Amendment (Computer Programs) Act 1999* (Cth) was passed into law on 24 August 1999.

### ***Copyright Amendment (Computer Programs) Act***

The *Copyright Amendment (Computer Programs) Act* was passed by Federal Parliament essentially as a precursor to the Digital Agenda reforms (as noted in Section 3.3.1). As outlined already in Section 2.5, the amendments added in entrenched rights for users of computer software:

- Make a back-up copy of the computer program;<sup>39</sup>
- Reproduce a computer program to make interoperable products;<sup>40</sup>
- Reproduce a computer program to correct errors;<sup>41</sup> and
- Reproduce a computer program for security testing;<sup>42</sup>

Importantly, these rights cannot be contracted away.<sup>43</sup> Any agreement which purports to do so is of no effect. The provisions concerning normal use, study and back-up were already discussed in Section 2.5, and will not be discussed further here.

### **Unauthorised use**

Section 47G is not a substantive provision, but provides that if a reproduction was permitted under a “prescribed provision” (one of the sections detailed below<sup>44</sup>), but<sup>45</sup>

---

<sup>39</sup> *Copyright Act 1968* (Cth) s 47C.

<sup>40</sup> *Copyright Act 1968* (Cth) s 47D.

<sup>41</sup> *Copyright Act 1968* (Cth) s 47E.

<sup>42</sup> *Copyright Act 1968* (Cth) s 47F.

<sup>43</sup> *Copyright Act 1968* (Cth) s 48H.

<sup>44</sup> *Copyright Act 1968* (Cth) s 47G(2).

<sup>45</sup> *Copyright Act 1968* (Cth) s 47G(1)(b).

the reproduction or adaptation, or any information derived from it, is, without the consent of the owner of the copyright in the computer program, used, or sold or otherwise supplied to a person, for a purpose other than a purpose specified in the prescribed provision

then the statutory protection does not apply, and, indeed is deemed never to have applied to the actions taken. The implications of this section are discussed in Section 5.2.1.

**Interoperability** Interoperable products are the basis of an open marketplace [24]. To allow a software vendor to establish a monopoly by refusing to allow a competitor to read and write the same files or otherwise communicate with it is an abuse of copyright (see Section 4.1.2). Yet, interoperability is one of the primary purposes cited when the virtues of reverse engineering are impugned.

The history of the greatest applications of computing is, in short, the history of standards [90]. The IBM Personal Computer flourished because any vendor could make hardware which was compatible with it. The Internet and the World Wide Web are based inexorably on open standards which allow the free exchange of data.<sup>46</sup> As such, interoperability is an important reason to examine and, if necessary, reverse engineer software.

Section 47D is an attempt to enshrine this into law, essentially adopting the “fair use” approach of the United States’ courts. Under section 47D, it is not an infringement to reproduce or make an adaptation of a computer program if:

1. the reproduction is made by a licensee of a copy of the program from a non-infringing copy;<sup>47</sup>
2. the reproduction or adaptation is made to gain necessary information to make an independently-written interoperable program;<sup>48</sup>

---

<sup>46</sup>The importance of this issue has recently been highlighted by the World Wide Web Consortium considering using patent-encumbered technology in upcoming standards. This attracted vehement opposition [64].

<sup>47</sup>*Copyright Act 1968* (Cth) s 47D(1)(a), (2).

<sup>48</sup>*Copyright Act 1968* (Cth) s 47D(1)(b).

3. the reproduction or adaptation is made only to the extent “reasonably necessary” to obtain the information<sup>49</sup> and it is not readily available from another source;<sup>50</sup> and
4. to the extent that the new, independently-written program contains information from the original program, it is only to the extent necessary to interoperate with the original program.<sup>51</sup>

This is, it can be noted, essentially the same test which was laid down in *Sega Enterprises Ltd. v. Accolade, Inc.*<sup>52</sup> (see Section 4.1.2). By applying section 47D to the facts of *Data Access Corporation v Powerflex Services Pty Ltd*,<sup>53</sup> the applicability of the section can be seen.

If *Powerflex* was to be decided today, the result would be wholly in favour of Powerflex. Where the High Court decided in favour of Powerflex on the basis of copyright law simpliciter, those results would obviously stand. Additionally, section 47D would also protect the Huffman compression table feature in PFXplus:

to the extent that the new program reproduces or adapts the original program, it does so only to the extent necessary to enable the new program to connect to and be used together with, or otherwise to interoperate with, the original program or the other program;

To the extent that PFXplus incorporated the Huffman compression table from Dataflex, it did so only to the extent necessary to enable PFXplus (which was quite clearly independently written) to interoperate with Dataflex: to read files saved by Dataflex with the compression feature turned on. (It is not necessary that the Huffman table itself be a computer program, only that it is incorporated into a computer program and essential to the effective operation of a function of the computer program.<sup>54</sup>)

---

<sup>49</sup> *Copyright Act 1968* (Cth) s 47(1)(c).

<sup>50</sup> *Copyright Act 1968* (Cth) s 47(1)(e).

<sup>51</sup> *Copyright Act 1968* (Cth) s 47(1)(d).

<sup>52</sup> 977 F.2d 1510 (9th Cir. 1992).

<sup>53</sup> (1999) 202 CLR 1; 166 ALR 228; 45 IPR 353; [1999] HCA 49 (30 September 1999).

<sup>54</sup> *Copyright Act 1968* (Cth) s 47AB.

If section 47D was applied to the facts of *Autodesk Inc v Dyason*, the section would permit the interoperability, but the Auto Key Lock would probably be a circumvention device, making selling it a civil and criminal offence (see Section 3.3.1).

Additionally, the actions leading to the creation of DeCSS would also seem to be protected in Australia (see Section 4.3.1). Section 47D merely requires that the reproduction or adaptation be made “for the purpose” of obtaining information necessary to create an interoperable product. The United States’ legislation requires the actions to be for the sole purpose of creating an interoperable product.<sup>55</sup>

**Error correction** It is also sensible to allow the reproduction of a copyrighted work in order to correct errors in the software. Indeed, when the Year 2000 (or Y2K) crisis was at its peak, it was suggested that, in some circumstances, correcting any Y2K-based errors would be a breach of copyright. Section 47E is an attempt to alleviate any such concern. Under that section, any reproduction or adaptation of a computer program<sup>56</sup>

made for the purpose of correcting an error in the original copy that prevents it from operating (including in conjunction with other programs or with hardware):

- (i) as intended by its author; or
- (ii) in accordance with any specifications or other documentation supplied with the original copy; and

The reproduction must only be to the extent necessary to correct the error,<sup>57</sup> and the copy modified must not be an infringing copy.<sup>58</sup>

The particular provisos in this case are important and deserve further examination. They establish that not all undesired behaviour is an error. However, it does ensure that the most obvious bugs can be fixed by the

---

<sup>55</sup>17 U.S.C. § 1201(f).

<sup>56</sup>*Copyright Act 1968* (Cth) s 47E(1)(b).

<sup>57</sup>*Copyright Act 1968* (Cth) s 47E(1)(c)

<sup>58</sup>*Copyright Act 1968* (Cth) s 47E(2).

user of the computer software if the software vendor is unable or unwilling to do so. Indeed, self-correction is only available if the vendor does not make the update available in reasonable time at an ordinary commercial price.<sup>59</sup>

Consider the situation where company *C* is using software product *P*, version *x*, running on operating system *O*, version *i*. *P* version *x* has a bug which *C* wants to correct. The vendor of product *P* has released version *x* + 1 which does not exhibit the bug, however it only runs on operating system *O* versions *i* + 1 and above. Does the availability of version *x* + 1 at an “ordinary commercial price” vitiate *C*’s rights under s 47E?

After all, when *C* would want to correct the error, another copy of the *P* that doesn’t exhibit the bug is available to *C* within a reasonable time at an ordinary commercial price. However, the provision of paragraph (b) may allow *C* to do its own in-house error correction. Paragraph (b), as extracted above, extends the notion of “error” to include the program’s operation with other programs. In the hypothetical above, version *x* + 1 of *P* does not “operate as mentioned in paragraph (b)” as it does not operate in conjunction with another program, namely *O* version *i*.

This limits the situations where a software vendor can force users of old software to new versions that require concomitant upgrades of other software or hardware—if the new version is not a “drop in” replacement, then the licensee can correct the program themselves.<sup>60</sup> This has obvious relevance (and brings glad tidings) to users and maintainers of legacy systems.

**Security testing** The permission to reproduce or adapt computer programs for the purpose of security testing is important. Nowhere is this more apparent than when computers are connected to the Internet. Even software written for the express purpose of robust handling of network input may have subtle errors which, when exploited, can cause damage.

---

<sup>59</sup>*Copyright Act 1968* (Cth) s 47E(1)(d).

<sup>60</sup>The wording of section 47E(1)(a) allows a software licensee to outsource this work. The reproduction or adaptation must be made “by, or on behalf of, the owner or licensee of the copy of the program”.

Section 47H is an attempt to balance the need for computer security researchers to examine software in depth (including using decompilation and other reverse engineering techniques) and yet ensure that nefarious persons cannot avail themselves of the protection.

The usual restrictions apply: the reproduction must be made “by, or on behalf of” the licensee of a non-infringing copy of the program.<sup>61</sup> The section protects any reproduction or adaptation made for the purpose of:<sup>62</sup>

- (i) testing in good faith the security of the original copy, or of a computer system or network of which the original copy is a part; or
- (ii) investigating, or correcting, in good faith a security flaw in, or the vulnerability to unauthorised access of, the original copy, or of a computer system or network of which the original copy is a part

As with the interoperability section, the actions need only be for “the purpose” (not the sole purpose) of testing or investigating security. One can also note the use of the words “in good faith” in both of the limbs of paragraph (b). This limits the people who can rely on the section to computer security researchers and others. The reproduction or adaptation of the computer program must be “by, or on behalf of, the owner or licensee of the copy”.<sup>63</sup> Additionally, the computer program must not be an infringing copy.<sup>64</sup> This allows for the security testing of legitimately-bought software (the term “security” is left undefined, though—the extent of the term could be somewhat nebulous).

Importantly, for the section to apply:<sup>65</sup>

the information resulting from the making of the reproduction or adaptation is not readily available to the owner or licensee from another source when the reproduction or adaptation is made.

---

<sup>61</sup>*Copyright Act 1968* (Cth) s 47F(1)(a), (2).

<sup>62</sup>*Copyright Act 1968* (Cth) s 47F(b).

<sup>63</sup>*Copyright Act 1968* (Cth) s 47F(1)(a).

<sup>64</sup>*Copyright Act 1968* (Cth) s 47F(2).

<sup>65</sup>*Copyright Act 1968* (Cth) s 47F(1)(d).

The operation of the section can be illustrated by examining hypothetical situations:

- A person, *A*, would like a third-party assessment of the security of software she has invested a large sum of money in, *S*. Although the vendor of the software *V* assures them the software is secure from a wide variety of attacks, *A* wants *B* to perform an evaluation.

After a thorough evaluation, including decompilation of fragments of the code in *S*, *B* concludes that the software is secure against a number of attacks. This coincides with the report which was given by *V* to *A*. As the information resulting from the making of the reproductions and adaptations of the software was readily available to *A*, *B* is not protected under section 47F.

An alternate argument would be that the decompilation is protected because the intermediate information which enabled the conclusion that the program was secure was not available to *A*, only the ultimate conclusion. On this basis, an argument could be made that the reverse engineering was permissible.

- A person, *A*, would like to check a commercial software product, *P*, for security vulnerabilities. If it is a good faith investigation, then any reproduction (including reverse engineering) for that purpose is protected.

Any malicious intent on the part of the tester, however, would appear to vitiate the legality of the investigation.

- A person, *A*, receives a copy of a file believed to be (or contain) a virus, worm or some other form of malicious software. In order to decide whether, and if so to what extent, the file is a security threat.

If the file is a self-contained worm, then even though the investigation may be for security research in good faith any reproduction may be a technical breach of copyright. This is because the section does not apply if the copy being reproduced is an infringing copy of the

computer program, nor if the research is not by or on behalf of the copyright holder of the program or a licensee.

In a practical sense, this is unlikely to be a problem—the copyright holder would need to identify him or herself in order to bring an action for copyright infringement. This would probably lead to proceedings against the copyright holder (possibly even criminal action). Nonetheless, the operation of section 47G remains a lingering concern to any such work.

It's also necessary to note that section 47F does not apply where the information gleaned from the inquiry is "readily available" to the owner or licensee of the computer software when the reproduction or adaptation was made.<sup>66</sup> Additionally, only reproductions or adaptations which are reasonably necessary are protected.<sup>67</sup>

## 4.2 Peer-to-peer networks

Peer-to-peer networking (or "P2P") has been widely adopted in recent times. A contextual definition is [99]:

On the Internet, peer-to-peer ... is a type of transient Internet network that allows a group of computer users with the same networking program to connect with each other and directly access files from one another's hard drives. Napster and Gnutella are examples of this kind of peer-to-peer software. Corporations are looking at the advantages of using P2P as a way for employees to share files without the expense involved in maintaining a centralized server and as a way for businesses to exchange information with each other directly.

Peer-to-peer networking is fundamentally different to the traditional model of networking: client-server or master-slave. In a peer-to-peer model, all machines in the network are essentially of equal status and

---

<sup>66</sup>*Copyright Act 1968* (Cth) s 47F(1)(d).

<sup>67</sup>*Copyright Act 1968* (Cth) s 47F(1)(c).

any can initiate connections with any other. This model of networking, as alluded to in the definition, has been used to facilitate file sharing over the Internet. The most prominent example of this was Napster. Napster enabled the sharing of music between Internet users on an unprecedented scale, and in so doing polarised the Internet populace. Internet users loved it, record companies hated it. Some artists decried it, others enthused about it [59].

Enthusiasm, the epitaph for Napster may well read, is no substitute for reality. The reality for Napster was that they were skating on perilously thin legal ice and even the famed advocacy of David Boies were not enough to save it. After losing the legal battle for its existence, Napster made peace with the record companies on the other side of the courtroom and reinvented itself as a subscription service.

#### 4.2.1 Napster

To understand the phenomenon of Napster, one must first understand the phenomenon of MP3. “MP3” stands for Motion Picture Expert Group (MPEG) Format 1 Layer 3, a standard for the lossy compression of audio data. The MP3 format is tailored for computationally inexpensive decompression at the expense of a computationally expensive one-time encoding. What made the MP3 standard popular was that it did a good job.<sup>68</sup> A single could be encoded at a rate which provided similar-to-radio quality in about 3 or 4 megabytes—easily transferred over a high-speed LAN or a fast modem link.

Shawn Fanning was one who recognised the potential of file swapping. Napster was originally software which he wrote which provided a directory of files which people wanted to make available to “share” with others. As such, networks of song traders grew in college dormitories. The idea proved to be popular and Napster, Inc., emerged. Napster’s central

---

<sup>68</sup>What may make the MP3 standard unpopular in the future is that the MP3 standard is not unencumbered. The Fraunhofer Institute holds patents necessary to encode an MP3 file, the use of which require a royalty payment. An alternative, unencumbered audio format—Ogg Vorbis—has been developed: <<http://www.vorbis.com/>>.

servers registered computers sharing files and provided a search facility. Client software made this readily accessible.

Such rabid music swapping couldn't go ignored by the music companies (the owners of the copyright in the music), and thus the Napster litigation began.<sup>69</sup>

Before Chief Judge Marilyn Hall Patel of the United States District Court for the Northern District of California, Napster was comprehensively defeated.<sup>70</sup> Chief Judge Patel found that, as a matter of fact, Napster caused significant economic damage to the record companies.<sup>71</sup>

Chief Judge Patel rejected the argument that Napster was engaging in fair use of the copyrighted music passing through its servers, as Napster provided for wholesale copying of the copyrighted works, and caused economic harm to the copyright owners.<sup>72</sup> The Napster service was distinguished from listening in a CD sampling booth because users kept copies of the music they were listening to.<sup>73</sup> Even the "substantial non-infringing uses" argument of *Sony* failed, as the non-infringing uses of Napster were held to be insubstantial.<sup>74</sup>

After holding that Napster users were probably engaging in direct copyright infringement, Chief Judge Patel further held that Napster was liable for contributory infringement because of the encouragement and contribution of Napster to the copyright infringements.<sup>75</sup> Napster was even, notwithstanding no employment relationship, vicariously liable because it had a financial interest in the copyright infringement.<sup>76</sup> Defences

---

<sup>69</sup>See *A & M Records, Inc. v. Napster, Inc.*, No. C 99-05183 MHP, 2000 U.S. Dist. LEXIS 6243, at \*1; 54 U.S.P.Q.2d (BNA) 1746 (May 5, 2000) ("On December 6, 1999, plaintiff record companies filed suit alleging contributory and vicarious federal copyright infringement and related state law violations by defendant Napster, Inc.")

<sup>70</sup>*A & M Records, Inc. v. Napster, Inc.*, 114 F. Supp. 2d 896 (N.D. Cal. 2000).

<sup>71</sup>*Napster*, 114 F. Supp. 2d at 909–11.

<sup>72</sup>*Napster*, 114 F. Supp. 2d at 912–13.

<sup>73</sup>*Napster*, 114 F. Supp. 2d at 913–14.

<sup>74</sup>*Napster*, 114 F. Supp. 2d at 916–17.

<sup>75</sup>*Napster*, 114 F. Supp. 2d at 918–920.

<sup>76</sup>*Napster*, 114 F. Supp. 2d at 920–922.

based on First Amendment,<sup>77</sup> copyright misuse<sup>78</sup> and waiver<sup>79</sup> were given short shrift.

On appeal, the Court of Appeals for the Ninth Circuit upheld the record companies' arguments on the same grounds as the District Court.<sup>80</sup> The only change the Court of Appeals made to the District Court decision was to limit the scope of the injunction on Napster's behaviour. The Court of Appeals put the burden on the record companies to identify copyrighted content on Napster's systems and for Napster to then remove the content upon notice from the record companies.<sup>81</sup>

Faced with almost-complete defeat, Napster is attempting to settle with the record companies and re-invent itself as a pay service [55, 56, 91]. It remains to be seen whether Internet users will pay for such a privilege.

#### 4.2.2 MP3.com

Other music distribution networks have been, and remain, in the sights of the record industry [54]. Although not a case of peer-to-peer networking, one case that went to trial was *UMG Recordings, Inc. v. MP3.com, Inc.*<sup>82</sup> The litigation concerned the "My.MP3.com" service offered by MP3.com. MP3.com bought thousands of CDs and, without any authorisation, created MP3 files of the music tracks on the CDs. By using the "Beam It Service" provided by MP3.com, a person could put an audio CD in their drive for a few seconds and if MP3.com had the CD in its catalogue, the MP3s from that CD would be added into the user's "locker". The MP3s could then be played by that user from wherever that user had an Internet connection.

Importantly for the copyright analysis employed by the court, the music which was broadcast to users was not a reproduction of music from their own CDs. It was a copy which had been created by MP3.com. A

---

<sup>77</sup>*Napster*, 114 F. Supp. 2d at 922–23.

<sup>78</sup>*Napster*, 114 F. Supp. 2d at 923.

<sup>79</sup>*Napster*, 114 F. Supp. 2d at 923–25.

<sup>80</sup>*A & M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001).

<sup>81</sup>*Napster*, 239 F.3d at 1027–28.

<sup>82</sup>92 F. Supp. 2d 349 (S.D.N.Y. 2000).

*prima facie* case of copyright infringement was made out but MP3.com argued the defence of fair use. The defence was rejected by Judge Rakoff, who began his judgment memorably:<sup>83</sup>

The complex marvels of cyberspatial communication may create difficult legal issues; but not in this case.

A fair use analysis showed that MP3.com was commercially profiting from unauthorised reproductions of the plaintiffs' copyrighted works. Although it was argued that this was primarily a means of "space shifting" music recordings already legally acquired by the users of the service, "[c]opyright ... is not designed to afford consumer protection or convenience but, rather, to protect the copyright holders' property interests."<sup>84</sup>

The strict legal analysis applied in the *MP3.com* case has clear implications for other innovative content distribution methods. Importantly, it means that equivalent behaviours will not be protected equally by the law—courts may tend to a microscopic rather than macroscopic analysis. In the *MP3.com* case, the effect to the user was the same as if they had taken their CD collection with them and were listening to CDs from that collection. Indeed, it would have been the same as making MP3s from their CD collection, putting it on a portable MP3 player and listening to that.<sup>85</sup> Yet because the My.MP3.com service involved the commercial, essentially unadulterated reproduction of music by MP3.com, the service fell outside the ambit of fair use.

### 4.2.3 Other P2P networks

After the Napster decision, Electronic Frontier Foundation attorney and Berkeley academic Fred von Lohmann wrote a white paper about the impact of copyright law on peer-to-peer networks [97]. In order to stay on the right side of copyright law, Professor von Lohmann essentially advises

---

<sup>83</sup>*MP3.com*, 92 F. Supp. 2d at 350.

<sup>84</sup>*MP3.com*, 92 F. Supp. 2d at 352.

<sup>85</sup>See *Recording Industry Association of America, Inc. v. Diamond Multimedia Systems, Inc.*, 180 F.3d 1072 (9th Cir. 1999).

network designers to maintain plausible deniability.<sup>86</sup> By having no control over the content passing through the network, no commercial interest in the success of the network and ensuring the network has substantial uses apart from the infringement of copyright, legal liability is difficult to establish.

### 4.3 Technological protection measures

While *ex post* legal action provides one remedy for copyright infringement or any other illegal act, it is not a complete solution. Legal action is expensive, and civil actions against impecunious plaintiffs are usually a waste of time. A far more seductive solution for rights holders is to prevent, by some technological means, the unwanted copying in the first place. A lesser adjunct would be to embed some form of identifying information in the material which would establish that a person had exceeded the copying permission.

If an effective technological protection regime could be implemented (this is expressly contemplated by the WCT), then legal protections would almost become moot. Record companies could distribute their music electronically without worrying about widespread piracy; movie studios could do likewise.

Indeed, some believe that copyright is not under threat but is instead at its apogee. With the advent of technologies such as trusted systems, it can be argued that copyright has been perfected [60].

#### 4.3.1 Encryption schemes

An important component of secure delivery of digital data is the use of encryption schemes to remove the ability to access the data without authorisation. These schemes are protected as technological protection measures by the legislation examined in Chapter 3 and the legal consequences of circumventing the encryption schemes is shown by two examples.

---

<sup>86</sup>With apologies to the Cigarette Smoking Man from *The X-Files*.

## DeCSS

The discussion of Napster may have suggested that the music industry was the only intellectual property industry which was under threat. Not so. With the unleashing of DeCSS, the motion picture industry also got very scared very quickly. The motion picture industry supported the widespread use and deployment of Digital Video Discs (DVDs). A DVD holds more than a CD; an entire movie—and extra bonus features—can be encoded on a single disc. The video and audio could also be digitally enhanced: appealing for people with home cinemas.

**The technology** Data on a DVD is encrypted using an “incompetently designed stream cipher known as Content Scrambling System (CSS)” [95]. The DVD Copy Control Authority (DVD CCA) would be responsible for handing out keys to vendors of player hardware and software. The theory was that should a given key be compromised, it could be revoked in future DVD pressings, reducing the utility of the compromised player [6].

As well as stand alone DVD players, DVD drives were available for computers. Software DVD players were available for some operating systems, but not for Linux.<sup>87</sup> This motivated a project to write such a player, in the spirit of co-operation alluded to in Section 2.4.2. A stumbling block for this project was the decryption of the CSS-encrypted data. In September 2000, this barrier was overcome courtesy of Jon Johansen, a 15-year-old Norwegian. Johansen released onto the Internet code called DeCSS which decrypted CSS-encoded data. *Et voilà*, DVDs under Linux.

The discovery of the encryption algorithm and the ability to find keys to decrypt content at will had implications far beyond the mere ability to play DVDs on alternative operating systems. It meant that DVDs could be copied with digital precision, a feat previously thought impossible. Further, with the use of video compression, the content of the DVD could be

---

<sup>87</sup>Richard M. Stallman, head of the Free Software Foundation, urges that the term “Linux” refer only to the kernel and the complete system is more properly called “GNU/Linux”, to indicate the fact that most of the programs on the system are a part of the GNU project [88].

re-encoded to a size which would enable it to fit onto a single CD. This made DVD content a tradable commodity online.

**The litigation** The motion picture industry sued in the United States District Court for the Southern District of New York, claiming that DeCSS was a “circumvention device” within the meaning of the DMCA. The plaintiffs did not sue the manufacturers of DeCSS (who were unknown) but people who hosted the DeCSS code on Web sites or linked to it. The Court agreed with the plaintiff’s arguments,<sup>88</sup> and issued an injunction restraining the parties to the case from distributing DeCSS.<sup>89</sup>

**Effective control of access** Judge Kaplan first found that although CSS was not a strong cipher, it nonetheless effectively controlled access to DVDs within the meaning of the DMCA.<sup>90</sup> As the only purpose of DeCSS was to circumvent CSS, it was a *prima facie* violation of the circumvention provisions of the DMCA.<sup>91</sup>

**DMCA defences** The defendants’ primary defence was that DeCSS was not written to enable the piracy of DVD movies but to further the development of a DVD player under the Linux operating system.<sup>92</sup> However, contentions based on this argument failed. Primarily, this was because the defendants were trafficking in the circumvention device, not creating it. The traffickers did not do any reverse engineering, therefore could not avail themselves of the reverse engineering for interoperability exception.<sup>93</sup>

Even if they did author them, it could not be contended that the sole purpose of DeCSS was to enable a Linux DVD player to be created: DeCSS was developed and ran under Windows and, additionally, the development of DeCSS was held to be “an end in itself”.<sup>94</sup> The existence of these

---

<sup>88</sup> *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000).

<sup>89</sup> *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 346 (S.D.N.Y. 2000).

<sup>90</sup> *Reimerdes*, 111 F. Supp. 2d at 317–18.

<sup>91</sup> *Reimerdes*, 111 F. Supp. 2d at 318–19.

<sup>92</sup> *Reimerdes*, 111 F. Supp. 2d at 319.

<sup>93</sup> *Reimerdes*, 111 F. Supp. 2d at 320.

<sup>94</sup> *Reimerdes*, 111 F. Supp. 2d at 320.

subsidiary motivations vitiated the theoretical availability of the defence. Additionally, as noted in Section 3.2.1, any public disclosure of the information nullifies the availability of the defence.<sup>95</sup>

Likewise, none of the defendants were engaged in *bona fide* encryption research or security testing and could therefore not avail themselves of those exceptions.<sup>96</sup>

**Fair use** The defendants finally relied on fair use. DeCSS could, after all, be used to enable fair uses of material on DVDs which may not be possible with other DVD players. The DMCA, Judge Kaplan decided, had struck the balance of fair use in favour of upholding technological protection measures, “preventing lawful as well as unlawful uses of copyrighted material”.<sup>97</sup> The long-standing test of substantial non-infringing uses (see Section 5.3.1) was not applicable to the analysis.<sup>98</sup> Indeed, the “trafficking” prohibition even extended to linking to copies of the code on the Web.<sup>99</sup>

**First Amendment** Although the court found some support in the view that computer software is fundamentally expressive, it came to the view that the provisions of the DMCA did not offend the freedom of speech guaranteed by the First Amendment.<sup>100</sup> Further, the liability for linking to DeCSS is constitutional providing the defendants know that the software is a circumvention device, as was the case.<sup>101</sup>

**Appeals** The decision has been appealed. The appeal attracted wide attention, and Kathleen Sullivan, Dean of Stanford Law School, represented the appellants before the Court of Appeals for the Second Circuit [67]. At the time of writing, the appellate court had not yet delivered a decision.

---

<sup>95</sup>*Reimerdes*, 111 F. Supp. 2d at 320.

<sup>96</sup>*Reimerdes*, 111 F. Supp. 2d at 320.

<sup>97</sup>*Reimerdes*, 111 F. Supp. 2d at 322.

<sup>98</sup>*Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417, 443 (1984).

<sup>99</sup>*Reimerdes*, 111 F. Supp. 2d at 324–26.

<sup>100</sup>*Reimerdes*, 111 F. Supp. 2d at 332–33, 339.

<sup>101</sup>*Reimerdes*, 111 F. Supp. 2d at 341.

## Adobe eBooks

The first criminal prosecution under the DMCA is against a Russian programmer who developed software that circumvented the encryption of Adobe eBooks. Despite the manifest legitimate uses of the Advanced eBook Processor—to enable back-up copies of eBooks and to enable text-to-speech conversion to name but two—Dmitry Skylarov is facing five years imprisonment in a foreign jail for an act legal in his own country.

At the time of writing, Mr. Skylarov is released on bail after pleading not guilty. Adobe has dropped its support of the suit, but as a criminal prosecution the progress of the prosecution rests solely with the discretion of the United States Attorney for the Northern District of California. The indictment against Mr. Skylarov is available at [http://www.usdoj.gov/usao/can/press/assets/applets/2001\\_08\\_28\\_sklyarov\\_ind.pdf](http://www.usdoj.gov/usao/can/press/assets/applets/2001_08_28_sklyarov_ind.pdf).

The situation of Mr. Skylarov indicates the far-reaching nature of the DMCA. Mr. Skylarov is not accused of copyright infringement and, indeed there is no alleged use of Mr. Skylarov's software to engage in copyright infringement of eBooks [63]. Nonetheless, a *prima facie* criminal case has been established. Furthermore, it shows the extra-territorial reach of the trafficking provisions of the DMCA: although the development of the software was in Russia and the marketing was over the World Wide Web, Mr. Skylarov has fallen foul of United States legislation.

## Summary

It is clear from the above examples that encryption schemes, no matter how incompetent or flimsy the design (one of the Adobe eBook encryption schemes was based on ROT-13), the WCT-based laws will protect them as technological measures. It is the law, not the technology, which therefore provides the protection [78].

### 4.3.2 Watermarking

Watermarking is often used in conjunction with encryption schemes and other forms of online content distribution [4]. The aim of watermarking is to hide information in data in order to “protect the copyright of a product or to demonstrate its authenticity” [98]. Although it does not stop the reproduction of data, it can provide an evidence trail should unauthorised dealing be suspected or detected [71].

Watermarking techniques have been developed for the use with still digital images, digital video and rendered text. Recent discussions of watermarking techniques include [10, 43, 58, 100].

Information encoded in watermarks is protected by the laws outlined in Chapter 3 as rights management information. The removal, alteration or other modification of watermarks is forbidden by the WCT<sup>102</sup> and national legislation implementing it.

### 4.3.3 Trusted systems

Trusted systems are an integrated solution for managing the distribution of digitised, copyrighted data. Key elements of trusted systems are encryption schemes and watermarking. Batya Friedman, Peter H. Kahn, Jr., and Daniel C. Howe write [35]:

Common sense tells us that the barriers to trust are least inhibiting when the potential harm is minimal and the good will of the person(s) we trust is genuine ... Conversely, barriers to trust occur when there is potentially significant harm and not much good will from the person(s) we trust ...

Trusted systems are used where there is potentially significant harm and no goodwill from the persons whom the data is delivered to. This indicates that trusted systems have a high burden to surmount. Nevertheless, Professor Lessig suggests that trusted systems may, in fact, implement perfect copyright control [60]. Appropriately, they were originally

---

<sup>102</sup>Article 12.

developed at Xerox Palo Alto Research Center.

The concept underpinning trusted systems is that communication only takes place between “trusted” machines. The most accessible description of the technology was published by Mark Stefik, one of the primary architects of the idea, in the *Scientific American* [89]. The motivation for the work is:

[A]uthors and publishers cannot make a living giving away their work. It now takes only a few keystrokes to copy a paragraph, an entire magazine, a book or even a life’s work. Uncontrolled copying has shifted the balance in the social contract between creators and consumers of digital works to the extent that most publishers and authors do not release their best work in digital form.

Dr. Stefik accurately identifies a symptom of this fear—many publishers and authors do not release their best work, or the entirety of their work, in digital form. Trusted system-based frameworks have been enthusiastically adopted by industry with consortiums such as SDMI established [51].

To enforce the constraints on the distribution and use of data within a trusted system, digital rights management (DRM) is used. This involves expressing the permitted uses of a digital work in a machine-readable language. The “trust” in a trusted system framework comes from the fact that all machines are trusted to honour the commands and restrictions of the DRM faithfully [89].

Trusted system frameworks are protected by the laws outlined in Chapter 3 as technological measures and rights management information. The prohibition against circumventing controls imposed by the trusted systems can obviate lawful uses of information, for example fair use or fair dealing. This is considered in Section 5.4.

## 4.4 Academic research

Standard academic behaviour is to research issues and produce papers about the findings of the research. Where research is made into technological protection measures, however, the ability of academics to subsequently publish their research may be threatened.

### 4.4.1 In the United States

The issue first came to a head in the United States. The SDMI Consortium (see Section 4.3.3) in order to check the viability of differing watermarking measures, ran a “Hack SDMI” challenge. Professor Ed Felten together with other researchers from Princeton University, detailed their attacks on the SDMI watermarking measures in an academic paper [18] and sought to present it to a USENIX conference in April 2001 but were threatened with legal action by the Recording Industry Association of America and the Secure Digital Music Initiative [21].

Seeking to present their paper at another conference without legal reprisal, Professor Felten filed suit in the United States District Court for the District of New Jersey seeking a declaration that their paper was not a “technology . . . that . . . is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a [copyrighted] work . . . .”<sup>103</sup>

After Professor Felten filed suit, the Recording Industry Association America and the Secure Digital Music Initiative dropped their threats of legal action and argued that there was no dispute before the court. The District Court has not decided the matter yet, although it appears that at least in the case of Professor Felten and his team’s paper, there is no threat of legal action. Nonetheless, the spectre of legal suit lingers over academic research in the area of encryption technology and security research [65].

---

<sup>103</sup>17 U.S.C. § 1201(a)(2).

#### **4.4.2 In Australia**

In Australia, it is unlikely that similar action would arise. The prohibition in the *Copyright Act* extends only to circumvention devices and circumvention services.<sup>104</sup> An academic research paper can't be seen as a device facilitating the circumvention of any protection measure, neither is it performing a service.

#### **4.4.3 In the European Union**

The text of Article 6(1) of Directive 2001/29/EC is broad enough to sanction the regulation of academic research:

Member States shall provide adequate legal protection against the circumvention of any effective technological measures . . .

Although the Directive has not been implemented in any national legislation, it is not unreasonable to posit that the regulation of academic research may be part of "adequate legal protection against the circumvention" of effective technological measures. However without domestic legislation to implement the Directive, only the possibility of application to academic research is able to be discerned in the abstract.

#### **4.4.4 In the United Kingdom**

The phrasing of *Copyright, Patents and Designs Act 1988* (UK) section 296(1) is broad enough to cover the copy protected works which are available today. Likewise, the wording of paragraph (2)(b) is broad. It is possible that researchers like Professor Ed Felten would be covered by the wording: was the paper by the Princeton researchers "intended to enable or assist persons to circumvent that form of copy-protection", or was it merely for facilitating academic discussion? Does the intent need to be the predominant intent or merely an ancillary benefit? Is the test wholly subjective, or does it have an objective component?

---

<sup>104</sup>*Copyright Act 1968* (Cth) ss 10(1), 116A–D, 132.

There are, at this stage, no definitive answers to these questions and, as such, the United Kingdom law is vague and arguably applies to academic research.

# Chapter 5

## Analysis

From the applications described in Chapter 4, it is clear that the laws regulating allowable behaviours of computer software are not perfect. Even laws which have laudable objects have flaws in their implementation. This chapter explores possible improvements to the legal landscape of computer software.

### **5.1 Is copyright the appropriate protection for computer software?**

Copyright, as noted in Chapter 2, protects the expression of ideas, not ideas themselves. As such, copyright is typically not used to protect functional objects—patent protection is typically the more appropriate protection for that. During the late 1980s and early 1990s, there were suggestions that copyright protection for computer software was not wholly appropriate; indeed, it has been suggested that copyright protection stunts innovation in software development [44].

#### **5.1.1 Patent protection**

Computer software in addition to being expressive is also inherently functional [11]. The traditional intellectual property protection for functional items is patent protection. Patents are exclusive rights for a manner or

method of manufactured; awarded if the manner or method is novel or inventive. If a patent is awarded (when the application has been examined and found to be sufficiently novel and inventive), the term is shorter than patent protection (TRIPS requires a minimum term of twenty years<sup>1</sup>) but independent development is not a defence—the patent is a monopoly on the method.

It is unquestioned that computer programs can be protected by patent. Computer software is therefore one of the few species of intellectual products which can double-dip for intellectual property protection. Greg Aharonian, the closest that patent law gets to a celebrity [75], is strident in his preference of patent protection over copyright law [1]. Likewise, Dan L. Burk notes that United States courts “have struggled with the paradox of applying intellectual property protection that explicitly does not extend to functional items to an item that is primarily functional” [12].

With some modifications, it appears that patent law can be comprehensive and flexible enough to provide a useful protection for computer programs [11].

### 5.1.2 *Sui generis* protection

As computer programs are a unique combination of expression and functionality it is not unreasonable to suggest that compute programs are protected by a unique (or *sui generis*) form of intellectual property. This was suggested in [77].

The authors of [77] have significant amounts of credibility in both the law and computer science fields. In an exhaustive manifesto, they argued for a hybrid between patent and copyright protection: protection for a short period of time should be automatic (or nearly automatic); particularly innovative developments can have extended protection whereby the author can receive a revenue stream for the development. In this way, computer software would receive pragmatic and useful protection.

Despite the doctrinal and practical appeals of *sui generis* protection for

---

<sup>1</sup>Article 33.

computer programs, copyright protection is deeply entrenched in international and national law and, as such, is not likely to ever be implemented, despite recent well-considered opinion that it may be worth reconsideration [11].

### 5.1.3 Software as speech

In the United States, the First Amendment to the Constitution (when read with the Ninth, Tenth and Fourteen Amendments) guarantees freedom of speech. Speech can only be regulated if there is a compelling governmental or social interest. Recent appellate court decisions in the United States have held that computer program code may indeed be speech [12, 74, 94].<sup>2</sup> (In Australia, this is less of an issue as the only freedom of speech guaranteed by the Australian Constitution is an implied freedom of political communication.<sup>3</sup>)

This orthodoxy has been challenged by recent decisions of courts in the United States suggesting that, at least to some extent, computer software in source code form can be protected speech.<sup>4</sup> This suggestion has been followed by academics such as Brian Fitzgerald and Lawrence Lessig.

In his articles [27, 28, 29], Dean Fitzgerald, building upon the work of postmodernist philosophers including Jacques Derrida and Michel Foucault, notes that “the quintessential element of discourse, of language, of speech, in this information society is software” [27]. In the emerging information society, Dean Fitzgerald argues, it is software which will become the dominant form of discourse. Private law, rather than public law, is becoming “new constitutionalism”—intellectual property, contract and competition and privacy law are, Dean Fitzgerald posits, more important than governmental and constitutional law. As such, the constitutional need to be re-examined to account for the new form of discourse.

---

<sup>2</sup>In a case currently before the Supreme Court of the United States, whether computer-generated data can attract First Amendment protection is the issue before the Court [34]. If computer-generated data attracts First Amendment protection, an extension to other computer data can be made.

<sup>3</sup>*Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520; 145 ALR 96.

<sup>4</sup>See, e.g., *Junger v. Daley*, 209 F.3d 481 (6th Cir. 2000).

In a similar vein, Professor Lessig recognises that code is the new form of regulation. It is code which is increasingly defining the constraints of our interactions. As such, code should be considered an arm of governmental regulation, subject to popular oversight [60, 61, 62].

Strict First Amendment protection for computer software has been stridently criticised [1, 11], but this misunderstands the thrust of the arguments of Dean Fitzgerald and Professor Lessig. The primary purpose of their discussions is not to suggest a solution or an approach, but to explicate the ubiquity of computer software in the modern world and to suggest that a political decision needs to be made with this ubiquity in mind [27, 60].

## **5.2 Could copyright protection for computer programs be improved?**

For the most part, the protection for computer programs is adequate. (This was not always the case—in Australia, the ability to create interoperable software was significantly curtailed for a long period of time [24].)

Despite the improvement, some of the exceptions to copyright infringements are drafted in a myopic manner: although the drafting seems to be sensible, it is not when applied to common factual scenarios.

### **5.2.1 Subsequent unauthorised use in Australia**

The reason this section was included is to discourage initial reproductions or adaptations being protected, but then used for impermissible purposes later.

This has the effect, however, of discouraging any dissemination of results gained from work which is protected. If research, say, for the normal use or study of a computer program is undertaken, the researchers cannot, say, give that information to assist someone attempting to create an interoperable product. This is despite the fact that both normal use and study and interoperability are separately protected purposes.

This is a significant legislative oversight. The requirement that the information must be “used, or sold or otherwise supplied to a person for a [different] purpose” should, however, protect most situations where information is published in academic journals. It remains, though, an unnecessarily vague part of the *Copyright Act*.

## 5.2.2 Can the guarantees be side-stepped?

Both in Australia and the United States, users of computer software have rights granted to them. If these guarantees can be—forgive the pun—circumvented, they are of little import. It does not appear that they can.

### In Australia

Brian Fitzgerald suggests that, despite the clear terms of section 47H of the *Copyright Act 1968* (Cth), an argument can be made for software vendors to restrict uses of their software, denying users the rights guaranteed by sections 47D to 47F (see Sections 2.5 and 4.1). Dean Fitzgerald argues [29]:

[A]s sections 47D–F are conditioned on the activities being undertaken by, or on behalf of, the owner or licensee of a copy of the program and on the copy of the software not being an infringing copy, there may be scope for arguing that the software manufacturer still has the capacity to license the product on terms that do not permit reverse engineering, thereby defeating sections 47D–F and circumventing 47H.

This argument, while inventive, does not appear to be supported by the wording of the legislation. If a software manufacturer attempts to take this approach, the license agreement for the software would need to have at least two provisions: the first allowing for the normal use of the software (otherwise the software would be, quite literally, useless) and the second forbidding reverse engineering. The second provision would be of no effect.<sup>5</sup> The copy of the software is not an infringing copy,<sup>6</sup> and it is

---

<sup>5</sup>*Copyright Act 1968* (Cth) s 47H.

<sup>6</sup>*Copyright Act 1968* (Cth) s 10(1).

not an infringement to reverse engineer the software for interoperability,<sup>7</sup> error correction<sup>8</sup> or security testing purposes.<sup>9</sup>

Simply put, the wording of section 47H is robust and forthright enough to cover the situation. Indeed, even where an agreement has the indirect effect of robbing a user of the rights granted by sections 47B(3) through 47F, the agreement will be of no effect because section 47H applies even where an agreement “has the effect of excluding or limiting” the rights.

### **In the United States**

The effect of similar actions in the United States is less clear. The Uniform Computer Information Transactions Act (UCITA). This is legislation proposed by the National Conference of Commissioners of Uniform State Laws for adoption by all States. Only Virginia and Maryland have adopted the UCITA into State law.

Although it has been argued that UCITA can effectively nullify the exceptions to copyright law [2, 53], the more legally rigorous approach seems to be that UCITA does not effect fair use rights or other provisions of copyright law [20, 33].

In any case, UCITA is currently under review by the American Bar Association [93]. The impact of UCITA on copyright protections may well change in response to the American Bar Association’s recommendations. Further, it has only been enacted in two States—its current impact is little.

## **5.3 Could the circumvention provisions be improved?**

Recent controversy has found its genesis in the circumvention provisions, primarily of the DMCA. As such, critical analysis of these provisions is apt.

---

<sup>7</sup>*Copyright Act 1968* (Cth) s 47D.

<sup>8</sup>*Copyright Act 1968* (Cth) s 47E.

<sup>9</sup>*Copyright Act 1968* (Cth) s 47F.

### 5.3.1 Are they necessary?

The circumvention provisions detailed in Chapter 3 were considered necessary to stop the rampant copying of digital data. Yet although an economic case can be made suggesting the threat is misplaced [5, 41], the circumvention provisions are part of legislation in the United States, Australia and the European Union.

#### Other forms of easily-copied data

The treatment given to computer data by the WCT and enacting legislation makes digital data a preferentially-treated species of copyrighted works. The legislation rests on the premise that the circumvention of technological protection measures equates to copyright infringement. This is, however, a false assumption from which to proceed [63]. First, technological protection measures may need to be circumvented merely in order to exercise rights guaranteed by law, such as fair use. Second, copyright infringement can be accomplished without needing to circumvent technological protection measures: by performing a raw copying of the media or by capturing the end product of the display.

Proponents of the WCT-type provisions may respond by arguing that computer data is substantively different from other forms of media and thus deserving of special protection. Computer data can be copied inexpensively and without degradation or loss. However, the issue of ease of copying is not a novel one—the spectre of backyard piracy has faced industries before, and it has come before the courts before.

**Anglo-Australian law** In Australia, any person who authorises, without a license, the doing of any act which the copyright owner has the exclusive right to do is liable as if that person directly infringed the copyright.<sup>10</sup> Indeed, authorising such acts is an exclusive right granted to the copyright holder.<sup>11</sup> To authorise an infringement is to sanction, approve or counte-

---

<sup>10</sup>*Copyright Act 1968* (Cth) ss 36(1), 101(1).

<sup>11</sup>*Copyright Act 1968* (Cth) s 13(2).

nance it.<sup>12</sup>

Authorisation was not proved where a journalist wrote an article about bootlegging audio recordings,<sup>13</sup> nor where blank tapes were advertised by using a recording artist's voice.<sup>14</sup> In the United Kingdom, manufacturers of high-speed tape-to-tape recorders were also protected from indirect infringement.<sup>15</sup>

**United States law** In the United States, the issue came before the courts in *Sony Corp. v. Universal City Studios, Inc.*<sup>16</sup> In *Sony*, Universal City Studios brought suit against Sony, manufacturer of the Betamax video recorder. Universal argued that consumers with the Betamax video recorder recorded television shows that Universal owned the copyright for thereby making an unauthorised reproduction. Further, Universal argued that because of how Sony advertised the Betamax recorder, it was liable for contributory infringement of copyright.

The Supreme Court of the United States held that<sup>17</sup>

the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses.

The Supreme Court found that noncommercial, private time-shifting (that is, the taping of a show at one time in order to watch it at another) was fair use and therefore noninfringing.<sup>18</sup> Together with the possibility of authorised time-shifting,<sup>19</sup> it was clear that the Betamax video recorder

---

<sup>12</sup>*University of New South Wales v Moorhouse* (1975) 133 CLR 1.

<sup>13</sup>*RCA Corporation v John Fairfax & Sons Ltd* (1981) 1 NSWLR 251; 34 ALR 345.

<sup>14</sup>*WEA International Inc v Hanimex Corporation Ltd* (1987) 17 FCR 274; 10 IPR 349.

<sup>15</sup>*CBS Songs Ltd v Amstrad Consumer Electronics plc* (1988) 11 IPR 1.

<sup>16</sup>464 U.S. 417 (1984). It is one of the ironies of copyright law that Sony was the defendant in this case, and, merely a decade and a half later, was a co-plaintiff with Universal City Studios in the Napster, MP3.com and DeCSS cases.

<sup>17</sup>*Sony*, 464 U.S. at 442.

<sup>18</sup>*Sony*, 464 U.S. at 451–56.

<sup>19</sup>*Sony*, 464 U.S. at 443–47.

was capable of substantial noninfringing uses. As such, Universal's action failed.<sup>20</sup>

**Summary** Despite blank tapes, high-speed tape recorders, video tape recorders and newspaper articles about copyright infringement being written, the recording and movie industries are still flourishing. Flagrant and mass piracy can still be punished with a direct infringement action. There was no suggestion that previous data should attract special copyright protection via the notion of technological protection measures. As such, the necessity and justification for the circumvention provisions detailed in Chapter 3 is not clear.

### 5.3.2 Defining a circumvention device

In Australia, a circumvention device is defined as being<sup>21</sup>

a device (including a computer program) having only a limited commercially significant purpose or use, or no such purpose or use, other than the circumvention, or facilitating the circumvention, of an effective technological protection measure.

While this provision may ostensibly seem reasonable, its application to open source software (see Section 2.4.2) is concerning. Open source software is often not sold; it is often distributed for no charge over the Internet.<sup>22</sup> Academic software is often distributed similarly—code is released freely by research groups.

Software distributed free of charge has, *prima facie*, no commercial purpose. There is no immediate commercial gain to the distributor (although some distributors may have a business plan involving selling service for the software).

---

<sup>20</sup>*Sony*, 464 U.S. at 456.

<sup>21</sup>*Copyright Act 1968* (Cth) s 10(1).

<sup>22</sup>See, for example, <http://www.freshmeat.net/> and <http://sourceforge.net/>.

This means that, in Australia, open source software or other software distributed for no immediate commercial gain which facilitates the circumvention of a technological protection measure will be a circumvention device, no matter how minor or incidental the circumvention is. This is because the software has no commercial purpose or use, let alone a commercial purpose or use other than circumventing the technological protection measures.

The obvious improvement is to omit the words “commercially significant”, like the analogous United States provision.<sup>23</sup> This does not detract from the meaning or purpose of the section, yet does not discriminate against open source and other non-commercial software.

### 5.3.3 Valé fair use and fair dealing?

In the United States, despite the lip-service paid to fair use in the text of the DMCA,<sup>24</sup> it is apparent that where data is protected by a technological protection measure, fair use is all but dead.<sup>25</sup>

In Australia, a similar process has occurred. Although Australia does not have a “fair use” provision based on the United States model (despite advocacy to that effect [26]), it does have a set of fair dealing provisions. Fair dealing with a copyrighted work for the purposes of research or study,<sup>26</sup> criticism or review,<sup>27</sup> or reporting news<sup>28</sup> is not an infringement of copyright. Yet it is not permissible to circumvent the technological protection on works for the purposes of fair dealing.<sup>29</sup>

The omission of these provisions in Australian law is surprising. Unlike the United States provisions which have only a handful of exceptions,<sup>30</sup> the Australian provision has a veritable surfeit of permissible pur-

---

<sup>23</sup>17 U.S.C. § 1201(a)(2)(A).

<sup>24</sup>17 U.S.C. § 1201(c). See Section 3.2.1.

<sup>25</sup>*Universal City Studios v Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000). See Section 4.3.1.

<sup>26</sup>*Copyright Act 1968* (Cth) s 40.

<sup>27</sup>*Copyright Act 1968* (Cth) s 41.

<sup>28</sup>*Copyright Act 1968* (Cth) s 42.

<sup>29</sup>*Copyright Act 1968* (Cth) s 116A(2). See Section 3.3.1.

<sup>30</sup>17 U.S.C. § 1201(c)-(j). See Section 3.2.1.

poses. Yet the fair dealing provisions are not among them. It is therefore not permissible for David Stratton to circumvent the technological protection on digital data in order to use a clip from a movie in a review, nor for a news organisation to circumvent technological protection in order to present a story on the evening news. This is a large lacuna in the legislation without an obvious justification and hence a lacuna which should be filled.

### 5.3.4 Intermediate copies in transit

The Australian provision that intends to protect Internet service providers from copyright infringement actions if they make intermediate copies of data in transit. However, this provision has two drafting problems.

#### Intermediate infringing copies

As noted in Section 3.3.1, intermediate copies made as part of the technical process of making or receiving a communication are protected.<sup>31</sup> The section does not apply where “the making of the communication is an infringement of copyright.”<sup>32</sup>

This, at first blush, seems reasonable. However the exclusion is too broad. The utility of section 43A(1) comes from the fact that facilitators of communication need not be worried about being the targets of copyright infringement actions. But subsection (2) negates this utility. Operators of proxy servers on the Internet may still be liable for the content of their proxies—if the original communication was an infringement of copyright (say, if it was pirated software or otherwise not for distribution) then keeping a copy in a proxy is likewise an infringement of copyright.

Accordingly, section 43A(2) should include a requirement of involvement or knowledge. A “knows, or has reason to know” caveat—much like that contained in the circumvention device provisions.<sup>33</sup>

---

<sup>31</sup>*Copyright Act 1968* (Cth) s 43A(1).

<sup>32</sup>*Copyright Act 1968* (Cth) s 43A(2).

<sup>33</sup>*Copyright Act 1968* (Cth) s 132(5A)–(5D).

## Caching proxy servers

Further, it is not clear whether optional reproductions (such as a caching or proxy server on the Internet) are covered. The statute only protects a “temporary reproduction . . . [made] as part as part of the technical process of making or receiving a communication”.<sup>34</sup> Where the making of a reproduction is not technically necessary, say with an proxy server provided by an Internet service provider, it is ambiguous as to whether the protection applies.

This shortcoming of the drafting should be rectified to protect any intermediate reproduction made automatically for technical reasons is not a breach of copyright. Such reproductions should be seen as part of the totality of network communication and therefore protected from being actionable as copyright infringement.

### 5.3.5 Recent legislative developments

As noted in Section 3.2.2, the Security Systems Standards and Certification Act (SSSCA) as recently been proposed in the United States. It has attracted the outrage of computing industry groups such as USENIX [3], the ACM [81] and the EFF [31]. Software vendors are likewise unimpressed [8, 83].

Bruce Schneier notes that the SSSCA “limits fair use, and basically puts the computer industry under the control of the entertainment industry” [79]. He also calls it “insane”. Eben Moglen, chief counsel for the Free Software Foundation, calls it “a deliberate attempt to destroy free software” [37].

The other concerning features of the Act are its broad definition of devices and the federal government blank-cheque approach to developing a standard [102]. This approach side-steps the existing plurality of competing standards in the marketplace today and, to the greatest extent possible, fortifies the position of the motion picture industry.

---

<sup>34</sup>*Copyright Act 1968* (Cth) s 43A(1).

Although this Act has not yet appeared in Congress and has not been the subject of any committee deliberations in either the House of Representatives or the Senate, the mere fact that this legislation has been credibly proposed suggests the level to which this issue has affected movie studios and other similar organizations. Indeed, on the Recording Industry Association of America's Web site, copyright is suggested to be a guaranteed right of authors of the same pre-eminence as Constitutionally guaranteed liberties [73]:

Before free speech, before freedom of assembly, before freedom of religion, there was copyright protection in our Constitution.

This is despite the fact that the constitutional authority of the federal government to grant copyrights is decidedly limited:<sup>35</sup>

The Congress shall have power . . . [t]o promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries . . .

The mere existence of proposed legislation in terms like the SSSCA demonstrates that copyright legislation which computing professionals find favourable does not appear to be a likely event. In order to ensure the continued legality of activities which computer scientists and other computing researchers customarily engage in, continued vigilance is necessary, and legislators must be educated.

## 5.4 Should a commons be legislated?

Trusted systems, as explored in Section 4.3.3, offer the potential for a far greater control over works than was previously allowed by copyright

---

<sup>35</sup>U.S. Const. Art. 1, § 8, cl. 8. This power has been interpreted liberally: see *Eldred v. Reno*, 239 F.3d 372 (D.C. Cir. 2001), rehearing denied, *Eldred v. Ashcroft*, 255 F.3d 849 (D.C. Cir. 2001).

laws. If all access to works can be regulated, then legal uses may be prohibited by copyright holders. In the words of James Boyle [9]:<sup>36</sup>

[T]he information superhighway will become an information toll road. The privatization of the public domain is unparalleled. Fair use rights will be cut back, individuals will be denied the right to give away copies of their digital works to their friends, even if they delete their own copies of those works. In fact ... even *reading* a document on the screen of your World Wide Web browser—without saving it to your floppy drive or hard disk—becomes a copyright violation!

This is a scary future—disturbingly plausible if trusted systems are allowed to propagate unchecked. To protect against this, some academics have suggested that a “commons” be established and protected by law. This would provide an oasis from the complete control that trusted systems could theoretically offer.

Currently, not only can trusted systems impose constraints on works antithetical to traditionally understood concepts of fair use and fair dealing, circumventing those copyright controls is illegal. The distribution of technologies which facilitate such circumventions is a civil and criminal offence, without proof of intent to breach the underlying copyright (see Chapter 3).

This near-future is conceivable, and it has given academics cause to worry [9, 29, 60]. It is eminently arguable that a future of perfect control of information is not in the wider public interest. It is certainly within the domain of governments to ensure that rights to which the public has grown accustomed to will not be taken away by technology.

However, the dystopian future of a world with perfect copyright control may never eventuate. Security experts consistently argue that trusted systems and other forms of technological control are doomed to failure [66, 78]. The Princeton team, led by Professor Ed Felten, who examined

---

<sup>36</sup>The quote, in its original context, discusses the “White Paper” on intellectual property rights on the National Information Infrastructure, released by the U.S. Government on September 5, 1995. The emphasis is in the original, and a footnote has been omitted.

the SDMI candidate watermarks (see Section 4.4.1) concluded their report thus [18]:

Do we believe we can defeat any audio protection scheme? Certainly, the technical details of any scheme will become known publicly through reverse engineering. Using the techniques we have presented here, we believe no public watermark-based scheme intended to thwart copying will succeed. Other techniques may or may not be strong against attacks. For example, the encryption used to protect consumer DVDs was easily defeated. Ultimately, if it is possible for a consumer to hear or see protected content, then it will be technically possible for the consumer to copy that content.

Ultimately, if a human experiences unencrypted content (or close enough to unencrypted content), then the content can be copied without the baggage of the technological protection measures [18, 66, 78]. This is perhaps the new balance (or, for want of a better term, fair use) to be struck in the digital world—perfect digital copies are facilitated through technological means such as trusted systems; copies less perfect but still adequate for most purposes can be taken at will [60].

Essentially this is a political judgment, however, to be made at a time when trusted systems are encroaching on the ability of copyright users to enjoy customary rights to works.

# Chapter 6

## Conclusion

### 6.1 Summary

This thesis has detailed the extensive protection granted by copyright law to computer programs and computer data. Applying these legal protections to not atypical computer science behaviours has shown the existence of tension between the protection of copyright law and uses of computer programs. Further, copyright law has elevated digitised data to a protected species. The circumvention provisions, finding their genesis in the WCT, have wider consequences than merely protecting digital data from widespread piracy.

### 6.2 Remedial action

As this thesis has demonstrated, there is a gulf between computer scientists and computer professionals on the one hand and legislators on the other. Legislative provisions are oftentimes not wholly suited to the technical issues that they are addressing. While computer scientists may bemoan the increasing influence that intellectual property has on their work, legislation affecting computer scientists—in some cases to their detriment—is still being proposed and being drafted [30, 84].

A dialogue needs to be established across the chasm of understanding

that separates the computing community from the legal community. An open discourse between the two sides will inform future actions on both sides and make future legislation and future political decisions in this area less problematic.

Adding an intellectual property course to the computer science curriculum is one way to accomplish this [15, 57]. Professor Donald S. Chisum suggests that one reason that the United States Supreme Court has made poor patent decisions is the low quality of scholarly writing in the area [13]. Legal education for computer scientists and better and more prevalent academic writing in the area can only lead to an improvement in the current situation. As was recently noted [57]:

One way to insure a more balanced debate on intellectual property issues in the future is to introduce computer science students to intellectual property concepts.

Conversely, the same reasoning suggests that it would be beneficial if legislators, judges and other such regulators became more computer-savvy. Some of the more startling decisions in intellectual property law are decided that way because of a fundamentally specious distinction about the technology [1].

As has been noted [9, 29, 60], computer software and computerised data are playing an increasingly important part in the fundamental interactions in today's world. It is timely and apt that computer scientists and legislators attempt to meet in the middle and develop a legally, technically and socially sound structure for future innovation.

### **6.3 Further research**

This thesis has attempted to fully describe the application of copyright law to computer software and computer data. There are several issues, ancillary to this thesis, which seem to suggest further research. On a purely technological basis, many of the technologies noted in this thesis (for example watermarking, trusted systems, digital rights management) are also

still being actively studied and refined by the commercial and academic spheres.

More eclectic is further research with both legal and computer science components.

- *Patents*: This thesis focused on copyright law and the application of copyright law to situations. Patent law also applies to computer programs, and a similar technological and comparative analysis could be performed for patent law and computer programs.
- *Doing it in reverse*: This thesis started with a discussion of the law and then applied it to conceivable applications of computer science. An reverse analysis—starting with a survey of computer science applications and determining their legality—would be useful. It has been consistently argued that the case-by-case exception approach of Australian law (and United States law vis-à-vis circumvention of technological protection measures) is not as flexible nor as durable as a broad fair use-based approach [26]. A reverse analysis should discover weaknesses in the legal case-by-case approach.
- *Legally robust networking*: Another practical research direction would be to critically analyse the infrastructure of peer-to-peer networks, and more conventionally structured networks, for legal liability. A corollary for this would be to design (or, from an existing network adapt a design) for a network with the lowest possible legal footprint; a network which is resistant to legal attacks.

The nexus between law and computer science is a dynamic one: law continually changes and technology continually advances. Copyright law has a far-reaching effect on the allowable uses of computer software and computer data; the scope of which will change as technology progresses and laws are refined.

# Appendix A

## International treaty provisions

### A.1 WIPO Performances and Phonograms Treaty

The WIPO Performances and Phonograms Treaty was adopted at Diplomatic Conference in Geneva from December 2 to 20, 1996. As of 22 October 2001, there were fifty signatories to the Treaty.

#### **Article 18**

(Obligations concerning Technological Measures)

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

#### **Article 19**

(Obligations concerning Rights Management Information)

- (1) Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty:

- (i) to remove or alter any electronic rights management information without authority;
  - (ii) to distribute, import for distribution, broadcast, communicate or make available to the public, without authority, performances, copies of fixed performances or phonograms knowing that electronic rights management information has been removed or altered without authority.
- (2) As used in this Article, “rights management information” means information which identifies the performer, the performance of the performer, the producer of the phonogram, the phonogram, the owner of any right in the performance or phonogram, or information about the terms and conditions of use of the performance or phonogram, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a fixed performance or a phonogram or appears in connection with the communication or making available of a fixed performance or a phonogram to the public.

# Appendix B

## European Union legislation

### B.1 Directive 91/250/EEC

Directive 91/250/EEC of the Council of European Communities of 14 May 1991 on the legal protection of computer programs.<sup>1</sup> It is available at <[http://europa.eu.int/eur-lex/en/lif/dat/1991/en\\_391L0250.html](http://europa.eu.int/eur-lex/en/lif/dat/1991/en_391L0250.html)>.

THE COUNCIL OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty establishing the European Economic Community and in particular Article 100a thereof,

Having regard to the proposal from the Commission,<sup>2</sup>

In cooperation with the European Parliament,<sup>3</sup>

Having regard to the opinion of the Economic and Social Committee,<sup>4</sup>

Whereas computer programs are at present not clearly protected in all Member States by existing legislation and such protection, where it exists, has different attributes;

Whereas the development of computer programs requires the investment of considerable human, technical and financial resources while computer programs can be copied at a fraction of the cost needed to develop them independently;

---

<sup>1</sup>Official Journal L 122, 17/05/1991 p. 0042–0046.

<sup>2</sup>OJ No C 91, 12.4.1989, p. 4; and OJ No C 320, 20.12.1990, p. 22.

<sup>3</sup>No C 231, 17.9.1990, p. 78; and Decision of 17 April 1991. Yet published in the Official Journal.

<sup>4</sup>OJ No C 329, 30.12.1989, p. 4.

Whereas computer programs are playing an increasingly important role in a broad range of industries and computer program technology can accordingly be considered as being of fundamental importance for the Community's industrial development;

Whereas certain differences in the legal protection of computer programs offered by the laws of the Member States have direct and negative effects on the functioning of the common market as regards computer programs and such differences could well become greater as Member States introduce new legislation on this subject;

Whereas existing differences having such effects need to be removed and new ones prevented from arising, while differences not adversely affecting the functioning of the common market to a substantial degree need not be removed or prevented from arising;

Whereas the Community's legal framework on the protection of computer programs can accordingly in the first instance be limited to establishing that Member States should accord protection to computer programs under copyright law as literary works and, further, to establishing who and what should be protected, the exclusive rights on which protected persons should be able to rely in order to authorize or prohibit certain acts and for how long the protection should apply;

Whereas, for the purpose of this Directive, the term "computer program" shall include programs in any form, including those which are incorporated into hardware; whereas this term also includes preparatory design work leading to the development of a computer program provided that the nature of the preparatory work is such that a computer program can result from it at a later stage;

Whereas, in respect of the criteria to be applied in determining whether or not a computer program is an original work, no tests as to the qualitative or aesthetic merits of the program should be applied;

Whereas the Community is fully committed to the promotion of international standardization;

Whereas the function of a computer program is to communicate and work together with other components of a computer

system and with users and, for this purpose, a logical and, where appropriate, physical interconnection and interaction is required to permit all elements of software and hardware to work with other software and hardware and with users in all the ways in which they are intended to function;

Whereas the parts of the program which provide for such interconnection and interaction between elements of software and hardware are generally known as “interfaces”;

Whereas this functional interconnection and interaction is generally known as ‘interoperability’; whereas such interoperability can be defined as the ability to exchange information and mutually to use the information which has been exchanged;

Whereas, for the avoidance of doubt, it has to be made clear that only the expression of a computer program is protected and that ideas and principles which underlie any element of a program, including those which underlie its interfaces, are not protected by copyright under this Directive;

Whereas, in accordance with this principle of copyright, to the extent that logic, algorithms and programming languages comprise ideas and principles, those ideas and principles are not protected under this Directive;

Whereas, in accordance with the legislation and jurisprudence of the Member States and the international copyright conventions, the expression of those ideas and principles is to be protected by copyright;

Whereas, for the purposes of this Directive, the term “rental” means the making available for use, for a limited period of time and for profit-making purposes, of a computer program or a copy thereof; whereas this term does not include public lending, which, accordingly, remains outside the scope of this Directive;

Whereas the exclusive rights of the author to prevent the unauthorized reproduction of his work have to be subject to a limited exception in the case of a computer program to allow the reproduction technically necessary for the use of that program by the lawful acquirer;

Whereas this means that the acts of loading and running necessary for the use of a copy of a program which has been law-

fully acquired, and the act of correction of its errors, may not be prohibited by contract; whereas, in the absence of specific contractual provisions, including when a copy of the program has been sold, any other act necessary for the use of the copy of a program may be performed in accordance with its intended purpose by a lawful acquirer of that copy;

Whereas a person having a right to use a computer program should not be prevented from performing acts necessary to observe, study or test the functioning of the program, provided that these acts do not infringe the copyright in the program;

Whereas the unauthorized reproduction, translation, adaptation or transformation of the form of the code in which a copy of a computer program has been made available constitutes an infringement of the exclusive rights of the author;

Whereas, nevertheless, circumstances may exist when such a reproduction of the code and translation of its form within the meaning of Article 4 (a) and (b) are indispensable to obtain the necessary information to achieve the interoperability of an independently created program with other programs;

Whereas it has therefore to be considered that in these limited circumstances only, performance of the acts of reproduction and translation by or on behalf of a person having a right to use a copy of the program is legitimate and compatible with fair practice and must therefore be deemed not to require the authorization of the rightholder;

Whereas an objective of this exception is to make it possible to connect all components of a computer system, including those of different manufacturers, so that they can work together;

Whereas such an exception to the author's exclusive rights may not be used in a way which prejudices the legitimate interests of the rightholder or which conflicts with a normal exploitation of the program;

Whereas, in order to remain in accordance with the provisions of the Berne Convention for the Protection of Literary and Artistic Works, the term of protection should be the life of the author and fifty years from the first of January of the year following the year of his death or, in the case of an anonymous or pseudonymous work, 50 years from the first of January of the year following the year in which the work is first published;

Whereas protection of computer programs under copyright laws should be without prejudice to the application, in appropriate cases, of other forms of protection; whereas, however, any contractual provisions contrary to Article 6 or to the exceptions provided for in Article 5 (2) and (3) should be null and void;

Whereas the provisions of this Directive are without prejudice to the application of the competition rules under Articles 85 and 86 of the Treaty if a dominant supplier refuses to make information available which is necessary for interoperability as defined in this Directive;

Whereas the provisions of this Directive should be without prejudice to specific requirements of Community law already enacted in respect of the publication of interfaces in the telecommunications sector or Council Decisions relating to standardization in the field of information technology and telecommunication;

Whereas this Directive does not affect derogations provided for under national legislation in accordance with the Berne Convention on points not covered by this Directive,

HAS ADOPTED THIS DIRECTIVE:

### **Article 1**

#### Object of protection

1. In accordance with the provisions of this Directive, Member States shall protect computer programs, by copyright, as literary works within the meaning of the Berne Convention for the Protection of Literary and Artistic Works. For the purposes of this Directive, the term 'computer programs' shall include their preparatory design material.
2. Protection in accordance with this Directive shall apply to the expression in any form of a computer program. Ideas and principles which underlie any element of a computer program, including those which underlie its interfaces, are not protected by copyright under this Directive.
3. A computer program shall be protected if it is original in the sense that it is the author's own intellectual creation. No other criteria shall be applied to determine its eligibility for protection.

## **Article 2**

### Authorship of computer programs

1. The author of a computer program shall be the natural person or group of natural persons who has created the program or, where the legislation of the Member State permits, the legal person designated as the rightholder by that legislation. Where collective works are recognized by the legislation of a Member State, the person considered by the legislation of the Member State to have created the work shall be deemed to be its author.
2. In respect of a computer program created by a group of natural persons jointly, the exclusive rights shall be owned jointly.
3. Where a computer program is created by an employee in the execution of his duties or following the instructions given by his employer, the employer exclusively shall be entitled to exercise all economic rights in the program so created, unless otherwise provided by contract.

## **Article 3**

### Beneficiaries of protection

Protection shall be granted to all natural or legal persons eligible under national copyright legislation as applied to literary works.

## **Article 4**

### Restricted Acts

Subject to the provisions of Articles 5 and 6, the exclusive rights of the rightholder within the meaning of Article 2, shall include the right to do or to authorize:

- (a) the permanent or temporary reproduction of a computer program by any means and in any form, in part or in whole. Insofar as loading, displaying, running, transmission or storage of the computer program necessitate such reproduction, such acts shall be subject to authorization by the rightholder;

- (b) the translation, adaptation, arrangement and any other alteration of a computer program and the reproduction of the results thereof, without prejudice to the rights of the person who alters the program;
- (c) any form of distribution to the public, including the rental, of the original computer program or of copies thereof. The first sale in the Community of a copy of a program by the rightholder or with his consent shall exhaust the distribution right within the Community of that copy, with the exception of the right to control further rental of the program or a copy thereof.

### **Article 5**

#### Exceptions to the restricted acts

1. In the absence of specific contractual provisions, the acts referred to in Article 4 (a) and (b) shall not require authorization by the rightholder where they are necessary for the use of the computer program by the lawful acquirer in accordance with its intended purpose, including for error correction.
2. The making of a back-up copy by a person having a right to use the computer program may not be prevented by contract insofar as it is necessary for that use.
3. The person having a right to use a copy of a computer program shall be entitled, without the authorization of the rightholder, to observe, study or test the functioning of the program in order to determine the ideas and principles 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**

#### Decompilation

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.

## **Article 7**

### Special measures of protection

1. Without prejudice to the provisions of Articles 4, 5 and 6, Member States shall provide, in accordance with their national legislation, appropriate remedies against a person

committing any of the acts listed in subparagraphs (a), (b) and (c) below:

- (a) any act of putting into circulation a copy of a computer program knowing, or having reason to believe, that it is an infringing copy;
  - (b) the possession, for commercial purposes, of a copy of a computer program knowing, or having reason to believe, that it is an infringing copy;
  - (c) 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.
2. Any infringing copy of a computer program shall be liable to seizure in accordance with the legislation of the Member State concerned.
  3. Member States may provide for the seizure of any means referred to in paragraph 1 (c).

### **Article 8**

#### Term of protection

1. Protection shall be granted for the life of the author and for fifty years after his death or after the death of the last surviving author; where the computer program is an anonymous or pseudonymous work, or where a legal person is designated as the author by national legislation in accordance with Article 2 (1), the term of protection shall be fifty years from the time that the computer program is first lawfully made available to the public. The term of protection shall be deemed to begin on the first of January of the year following the abovementioned events.
2. Member States which already have a term of protection longer than that provided for in paragraph 1 are allowed to maintain their present term until such time as the term of protection for copyright works is harmonized by Community law in a more general way.

### **Article 9**

#### Continued application of other legal provisions

1. The provisions of this Directive shall be without prejudice to any other legal provisions such as those concerning patent rights, trade-marks, unfair competition, trade secrets, protection of semi-conductor products or the law of contract. Any contractual provisions contrary to Article 6 or to the exceptions provided for in Article 5 (2) and (3) shall be null and void.
2. The provisions of this Directive shall apply also to programs created before 1 January 1993 without prejudice to any acts concluded and rights acquired before that date.

### **Article 10**

#### Final provisions

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive before 1 January 1993.  
When Member States adopt these measures, the latter shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such a reference shall be laid down by the Member States.
2. Member States shall communicate to the Commission the provisions of national law which they adopt in the field governed by this Directive.

### **Article 11**

This Directive is addressed to the Member States.

## **B.2 Directive 2001/29/EC**

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.<sup>5</sup> It is available at <http://europa.>

---

<sup>5</sup>Official Journal L 167, 22/06/2001 P. 0010–0019.

[eu.int/eur-lex/en/lif/dat/2001/en\\_301L0029.html](http://eu.int/eur-lex/en/lif/dat/2001/en_301L0029.html)> or  
<<http://www.eurorights.org/eudmca/CopyrightDirective.html>>.

## **Article 2**

### **Reproduction right**

Member States shall provide for the exclusive right to authorise or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part:

- (a) for authors, of their works;
- (b) for performers, of fixations of their performances;
- (c) for phonogram producers, of their phonograms;
- (d) for the producers of the first fixations of films, in respect of the original and copies of their films;
- (e) for broadcasting organisations, of fixations of their broadcasts, whether those broadcasts are transmitted by wire or over the air, including by cable or satellite.

## **Article 3**

### **Right of communication to the public of works and right of making available to the public other subject-matter**

1. Member States shall provide authors with the exclusive right to authorise or prohibit 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 them from a place and at a time individually chosen by them.
2. Member States shall provide for the exclusive right to authorise or prohibit the making available to the public, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them:
  - (a) for performers, of fixations of their performances;
  - (b) for phonogram producers, of their phonograms;
  - (c) for the producers of the first fixations of films, of the original and copies of their films;

- (d) for broadcasting organisations, of fixations of their broadcasts, whether these broadcasts are transmitted by wire or over the air, including by cable or satellite.
3. The rights referred to in paragraphs 1 and 2 shall not be exhausted by any act of communication to the public or making available to the public as set out in this Article.

...

### **Article 5**

#### Exceptions and limitations

1. Temporary acts of reproduction referred to in Article 2, which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable:
  - (a) a transmission in a network between third parties by an intermediary, or
  - (b) a lawful useof a work or other subject-matter to be made, and which have no independent economic significance, shall be exempted from the reproduction right provided for in Article 2.
2. Member States may provide for exceptions or limitations to the reproduction right provided for in Article 2 in the following cases:
  - (a) 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 rightholders receive fair compensation;
  - (b) 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 rightholders 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;

- (c) 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;
  - (d) 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;
  - (e) in respect of reproductions of broadcasts made by social institutions pursuing non-commercial purposes, such as hospitals or prisons, on condition that the rightholders receive fair compensation.
3. Member States may provide for exceptions or limitations to the rights provided for in Articles 2 and 3 in the following cases:
- (a) use for the sole purpose of illustration for teaching or scientific research, as long as the source, including the author's name, is indicated, unless this turns out to be impossible and to the extent justified by the non-commercial purpose to be achieved;
  - (b) 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;
  - (c) reproduction by the press, communication to the public or making available of published articles on current economic, political or religious topics or of broadcast works or other subject-matter of the same character, in cases where such use is not expressly reserved, and as long as the source, including the author's name, is indicated, or use of works or other subject-matter in connection with the reporting of current events, to the extent justified by the informative purpose and as long as the source, including the author's name, is indicated, unless this turns out to be impossible;
  - (d) quotations for purposes such as criticism or review,

provided that they relate to a work or other subject-matter which has already been lawfully made available to the public, that, unless this turns out to be impossible, the source, including the author's name, is indicated, and that their use is in accordance with fair practice, and to the extent required by the specific purpose;

- (e) use for the purposes of public security or to ensure the proper performance or reporting of administrative, parliamentary or judicial proceedings;
- (f) use of political speeches as well as extracts of public lectures or similar works or subject-matter to the extent justified by the informatory purpose and provided that the source, including the author's name, is indicated, except where this turns out to be impossible;
- (g) use during religious celebrations or official celebrations organised by a public authority;
- (h) use of works, such as works of architecture or sculpture, made to be located permanently in public places;
- (i) incidental inclusion of a work or other subject-matter in other material;
- (j) use for the purpose of advertising the public exhibition or sale of artistic works, to the extent necessary to promote the event, excluding any other commercial use;
- (k) use for the purpose of caricature, parody or pastiche;
- (l) use in connection with the demonstration or repair of equipment;
- (m) use of an artistic work in the form of a building or a drawing or plan of a building for the purposes of reconstructing the building;
- (n) use by communication or making available, for the purpose of research or private study, to individual members of the public by dedicated terminals on the premises of establishments referred to in paragraph 2(c) of works and other subject-matter not subject to purchase or licensing terms which are contained in their collections;

- (o) use in certain other cases of minor importance where exceptions or limitations already exist under national law, provided that they only concern analogue uses and do not affect the free circulation of goods and services within the Community, without prejudice to the other exceptions and limitations contained in this Article.
4. Where the Member States may provide for an exception or limitation to the right of reproduction pursuant to paragraphs 2 and 3, they may provide similarly for an exception or limitation to the right of distribution as referred to in Article 4 to the extent justified by the purpose of the authorised act of reproduction.
  5. 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 rightholder.

#### **Article 6**

##### Obligations as to protection measures

1. Member States shall 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.
2. 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, or
  - (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.

3. For the purposes of this Directive, the expression "technological measures" means any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the rightholder of any copyright or any right related to copyright as provided for by law or the sui generis right provided for in Chapter III of Directive 96/9/EC. Technological measures shall be deemed "effective" where the use of a protected work or other subject-matter is controlled by the rightholders 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.
4. Notwithstanding the legal protection provided for in paragraph 1, in the absence of voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, Member States shall take appropriate measures to ensure that rightholders make available to the 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 means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned.

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 reproduction for private use has already been made possible by rightholders 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 rightholders from adopting adequate measures regarding the number of reproductions in accordance with these provisions.

The technological measures applied voluntarily by rightholders, including those applied in implementation of voluntary agreements, and technological measures ap-

plied in implementation of the measures taken by Member States, shall enjoy the legal protection provided for in paragraph 1.

The 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 place and at a time individually chosen by them.

# Bibliography

- [1] Greg Aharonian. Deconstructing software copyright: 30 years of bad logic. <<http://www.bustpatents.com/aharonian/softcopy.htm>>, October 2001.
- [2] Americans for Fair Electronic Commerce Transactions. Why we oppose UCITA. <<http://www.4cite.org/why.html>>. Visited 31 October 2001.
- [3] USENIX Association. Proposed legislation significantly affecting computer profession. <<http://www.usenix.org/whatsnew/legislation.html>>. Visited 29 October 2001.
- [4] Daniel Augot, Jean-Marc Boucqueau, Jean-François Delaigle, Caroline Fontaine, and Eddy Goray. Secure delivery of images over open networks. *Proceedings of the IEEE*, 87(7):1251–1266, July 1999.
- [5] John Perry Barlow. The economy of ideas. *Wired*, 2.03, March 1994. <<http://www.wired.com/wired/archive/2.03/economy.ideas.html>>.
- [6] Jeffrey A. Bloom, Ingemar J. Cox, Ton Kalker, Jean-Paul M.G. Linnartz, Matthew L. Miller, and C. Brendan S. Traw. Copy protection for DVD video. *Proceedings of the IEEE*, 87(7):1267–1276, July 1999.
- [7] *The Bluebook: A Uniform System of Citation*. Harvard Law Review Association, Cambridge, Mass., U.S.A., seventeenth edition, 2000.
- [8] John Borland. Techs broadside anti-piracy plan. <<http://www.zdnet.com/zdnn/stories/news/0,4586,5098618,00.html>>. Visited 30 October 2001.
- [9] James Boyle. *Shamans, Software, and Spleens: Law and the Construction of the Information Society*. Harvard University Press, Cambridge, Mass., U.S.A., 1996.

- [10] Jack T. Brassil, Steven Low, and Nicholas F. Maxemchuk. Copyright protection for the electronic distribution of text documents. *Proceedings of the IEEE*, 87(7):1181–1196, July 1999.
- [11] Dan L. Burk. Patenting speech. *Texas Law Review*, 79:99–162, 2000.
- [12] Dan L. Burk. Copyrightable functions and patentable speech. *Communications of the ACM*, 44(2):69–75, February 2001.
- [13] Donald S. Chisum. The Supreme Court and patent law: Does shallow reasoning lead to thin law? <[http://www.ipmall.fplc.edu/hosted\\_resources/chisum.htm](http://www.ipmall.fplc.edu/hosted_resources/chisum.htm)>. Visited 30 October 2001.
- [14] Cristina Cifuentes. Reverse engineering and the computing profession. *Computer*, 2001. (Forthcoming).
- [15] Cristina Cifuentes and Anne Fitzgerald. Introducing a legal strand in the computer science curriculum. Technical Report 427, School of Information Technology, The University of Queensland, March 1998.
- [16] Thomas H. Cormen, Charles E. Leiserson, and Ronald L. Rivest. *Introduction to Algorithms*. The MIT Press, Cambridge, Mass., U.S.A., 1990.
- [17] Microsoft Corporation. End-user license agreement for windows 98. <<http://nl.linux.org/geldterug/license.html>>. Visited 30 October 2001.
- [18] Scott A. Craver, John R. McGregor, Min Wu, Bede Liu, Adam Stubblefield, Ben Swartzlander, Dan S. Wallach, Drew Dean, and Edward W. Felten. Reading between the lines: Lessons from the SDMI challenge. <<http://cryptome.org/sdmi-attack.htm>>, visited 30 October 2001.
- [19] Rod Dixon. When efforts to conceal may actually reveal: Whether first amendment protection of encryption source code and the open source movement support re-drawing the constitutional line between the first amendment and copyright. *Columbia Science and Technology Law Review*, 1:3, 2000.

- [20] Eric Douma. The Uniform Computer Information Transactions Act and the issue of preemption of contractual provisions prohibiting reverse engineering, disassembly, or decompilation. *Albany Law Journal of Science & Technology*, 11:249–285, 2001.
- [21] Electronic Frontier Foundation. Princeton scientists sue over squelched research. <[http://www.eff.org/Legal/Cases/Felten\\_v\\_RIAA/20010606\\_eff\\_felten\\_pr.htm%1](http://www.eff.org/Legal/Cases/Felten_v_RIAA/20010606_eff_felten_pr.htm%1)>. Visited 1 November 2001.
- [22] Eurorights.org, your rights online. <<http://www.eurorights.org/eudmca/>>. Visited 30 October 2001.
- [23] Michael B. Feldman and Elliot B. Koffman. *Ada 95: Problem Solving and Program Design*. Addison-Wesley, Reading, Mass., U.S.A., second edition, 1996.
- [24] Anne Fitzgerald and Cristina Cifuentes. Interoperability and computer software protection in australia. Technical Report 426, School of Information Technology, The University of Queensland, December 1997.
- [25] Anne Fitzgerald and Cristina Cifuentes. Copyright protection for digital multimedia works. In Anne Fitzgerald, Brian Fitzgerald, Peter Cook, and Cristina Cifuentes, editors, *Going Digital: Legal Issues for Electronic Commerce, Multimedia and the Internet*, pages 13–21. Prospect Media, St. Leonards, N.S.W., Australia, 1998.
- [26] Anne Fitzgerald and Cristina Cifuentes. Pegging out the boundaries of computer software copyright: The Computer Programs Act and the Digital Agenda Bill. In Anne Fitzgerald, Brian Fitzgerald, Cristina Cifuentes, and Peter Cook, editors, *Going Digital 2000: Legal issues for e-commerce, software and the internet*, pages 37–70. Prospect Media, St. Leonards, N.S.W., Australia, 2000.
- [27] Brian Fitzgerald. Software as discourse? A constitutionalism for information society. *Alternative Law Journal*, 24(3):144–149, June 1999.
- [28] Brian Fitzgerald. Software as discourse: The challenge for information law? *European Intellectual Property Review*, page 47, 2000.
- [29] Brian F. Fitzgerald. Software as discourse: The power of intellectual property in digital architecture. *Cardozo Arts & Entertainment Law Journal*, 18:337–386, 2000.

- [30] Electronic Frontier Foundation. EFF counsels New Zealand on copyright law revamp. <[http://www.eff.org/IP/Foreign\\_and\\_local/New\\_Zealand/20011023\\_eff\\_dpdtca%\\_pr.html](http://www.eff.org/IP/Foreign_and_local/New_Zealand/20011023_eff_dpdtca%_pr.html)>. Visited 30 October 2001.
- [31] Electronic Frontiers Foundation. Defeat the “Security Systems Standards and Certification Act”. <[http://www.eff.org/alerts/20010921\\_eff\\_sssca\\_alert.html](http://www.eff.org/alerts/20010921_eff_sssca_alert.html)>. Visited 29 October 2001.
- [32] Free Software Foundation. The free software definition. <<http://www.gnu.org/philosophy/free-sw.html>>. Visited 30 October 2001.
- [33] Garry L. Founds. Shrinkwrap and clickwrap agreements: 2B or not 2B? *Federal Communications Law Journal*, 52:99–123, December 1999.
- [34] Eric M. Freedman. Pondering pixelized pixies. *Communications of the ACM*, 44(8):27–29, August 2001.
- [35] Batya Friedman, Jr. Peter H. Kahn, and Daniel C. Howe. Trust online. *Communications of the ACM*, 43(2):34–40, December 2000.
- [36] Brett Frischmann and Dan Moylan. The evolving common law doctrine of copyright misuse: A unified theory and its application to software. *Berkeley Technology Law Journal*, 15:865–931, 2000.
- [37] Tina Gasperson. SSSCA gets a hearing Oct. 25—can it be stopped? <<http://www.newsforge.com/article.pl?sid=01/10/19/1546246>>. Visited 29 October 2001.
- [38] Karen E. Georgenson. Reverse engineering of copyrighted software: Fair use or misuse? *Albany Law Journal of Science and Technology*, 5:291–320, 1996.
- [39] William Gibson. *Neuromancer*. Grafton, London, U.K., 1986.
- [40] Robert W. Gomulkiewicz. How copyleft uses license rights to succeed in the open source software revolution and the implications for article 2b. *Houston Law Review*, 36:179–194, 1999.
- [41] Peter Grabosky, Russell G. Smith, and Gillian Dempsey. *Electronic Theft: Unlawful Acquisition in Cyberspace*. Cambridge University Press, Cambridge, U.K., 2001.

- [42] D. J. Harris. *Cases and Materials on International Law*, chapter 1, pages 1–14. Sweet & Maxwell, London, U.K., fifth edition, 1998.
- [43] Frank Hartung and Martin Kutter. Multimedia watermarking techniques. *Proceedings of the IEEE*, 87(7):1079–1107, July 1999.
- [44] Mark A. Haynes. Black holes of innovation in the software arts. *Berkeley Technology Law Journal*, 14:567–575, 1999.
- [45] Natasha T. Horne. Open source software licensing: Using copyright law to encourage fair use. *Georgia State University Law Review*, 17:873–891, 2001.
- [46] Adobe Systems Inc. Adobe Acrobat Reader 5 end user license agreement. <<http://www.adobe.com/products/acrobat/acrreula.html>>. Visited 30 October 2001.
- [47] Apple Computer Inc. Apple Computer, Inc. software license. <[http://store.apple.com/Catalog/US/Images/swlicense\\_apple.html](http://store.apple.com/Catalog/US/Images/swlicense_apple.html)>. Visited 30 October 2001.
- [48] Novell Inc. Novell eDirectory v 8.5 software license. <<http://developer.novell.com/edirectory/eula.pdf>>. Visited 30 October 2001.
- [49] Open Source Initiative. Open source definition. <<http://www.opensource.org/docs/definition.html>>. Visited 30 October 2001.
- [50] Open Source Initiative. OSI certification mark and program. <[http://www.opensource.org/docs/certification\\_mark.html](http://www.opensource.org/docs/certification_mark.html)>. Visited 30 October 2001.
- [51] Secure Digital Music Initiative. SDMI fact sheet. <[http://www.sdmi.org/who\\_we\\_are.htm](http://www.sdmi.org/who_we_are.htm)>. Visited 1 November 2001.
- [52] Paul Kalina and Pip Bulbeck. Video stores, Warner at war. <<http://www.theage.com.au/entertainment/2001/11/01/FFXWYDZYFTC.html>>. Visited 2 November 2001.
- [53] Cem Kaner. UCITA list of articles. <<http://www.badsoftware.com/uccindex.htm>>. Visited 31 October 2001.

- [54] Brad King. File trading sites in crosshairs. <<http://www.wired.com/news/mp3/0,1285,47296,00.html>>. Visited 1 November 2001.
- [55] Brad King. Good beat, but can't dance to all. <<http://www.wired.com/news/culture/0,1284,47401,00.html>>. Visited 1 November 2001.
- [56] Brad King. Napster settles, eyes relaunch. <<http://www.wired.com/news/mp3/0,1285,47075,00.html>>. Visited 1 November 2001.
- [57] John P. Kozma and Thomas Dion. An intellectual property course for cs majors. *Crossroads: The ACM Student Magazine*, 8(1):4–9, Fall 2001.
- [58] Deepa Kundur and Dimitrios Hatzinakos. Digital watermarking for telltale tamper proofing and authentication. *Proceedings of the IEEE*, 87(7):1167–1180, July 1999.
- [59] Calvin K.M. Lam and Bernard C.Y. Tan. The internet is changing the music industry. *Communications of the ACM*, 44(8):62–68, August 2001.
- [60] Lawrence Lessig. *Code and Other Laws of Cyberspace*. Basic Books, New York, N.Y., U.S.A., 1999.
- [61] Lawrence Lessig. The limits in open code: Regulatory standards and the future of the net. *Berkeley Technology Law Journal*, 14:759–769, 1999.
- [62] Lawrence Lessig. Open code and open societies: Values of internet governance. *Chicago-Kent Law Review*, 74:1405–1420, 1999.
- [63] Lawrence Lessig. Jail time in the digital age. *New York Times*, 30 July 2001.
- [64] Timothy Lord. W3C considers royalty-bound patents in Web standards. <<http://slashdot.org/article.pl?sid=01/09/30/1454216>>. Visited 31 October 2001.
- [65] Rob Malda. DMCA forces Cox to censor changelog? <<http://slashdot.org/yro/01/10/22/172200.shtml>>. Visited 1 November 2001.

- [66] Charles C. Mann. There's no such thing as "secure digital music". <<http://www.theatlantic.com/issues/2000/09/mann-farmer.htm>>. Visited 2 November 2001.
- [67] Declan McCullagh. Hackers vs. Hollywood, the sequel. <<http://www.wired.com/news/digiwood/0,1412,43450,00.html>>. Visited 30 October 2001.
- [68] Declan McCullagh. New copyright bill heading to DC. <<http://www.wired.com/news/politics/0,1283,46655,00.html>>. Visited 30 October 2001.
- [69] David McGowan. Intellectual property challenges in the next century: Legal implications of open-source software. *University of Illinois Law Review*, pages 241–304, 2001.
- [70] Jill McKeough and Andrew Stewart. *Intellectual Property in Australia*. Butterworths, Chatswood, N.S.W., Australia, second edition, 1997.
- [71] Fred Mintzer, Gordon W. Braudaway, Francis P. Giordano, Jack C. Lee, Karen A. Magerlein, Silvana D'Auria, Annon Ribak, Gil Shapir, Fabio Schiattarella, John Tolva, and Andrey Zelenkov. Populating the Hermitage Museum's new Web site. *Communications of the ACM*, 44(8):52–60, August 2001.
- [72] David Nimmer. A riff on fair use in the Digital Millennium Copyright Act. *University of Pennsylvania Law Review*, 148:673–742, 2000.
- [73] Recording Industry Association of America. What is copyright? <<http://www.riaa.com/Copyright-What.cfm>>. Visited 29 October 2001.
- [74] Robert Post. Encryption source code and the first amendment. *Berkeley Technology Law Journal*, 15:713–723, 2000.
- [75] Evan Ratliff. Patent upending. *Wired*, 8.06:206, June 2000. <<http://www.wired.com/wired/archive/8.06/patents.html>>.
- [76] Pamela Samuelson. Intellectual property for an information age. *Communications of the ACM*, 44(2):67–68, February 2001.
- [77] Pamela Samuelson, Randall Davis, Mitchell D. Kapor, and J.H. Reichman. A manifesto concerning the legal protection of computer programs. *Columbia Law Review*, 94:2308–2431, 1994.

- [78] Bruce Schneier. *Secrets and Lies: Digital Security in a Networked World*. John Wiley & Sons, New York, N.Y., U.S.A., 2000.
- [79] Bruce Schneier. Crypto-gram. <<http://www.counterpane.com/crypto-gram-0110.html>>, October 2001.
- [80] Brad Sherman and Lionel Bently. *The Making of Modern Intellectual Property Law: The British Experience, 1760–1911*. Cambridge University Press, Cambridge, U.K., 1999.
- [81] Barbara Simons and Eugene H. Spafford. Letter to Senator Ernest Hollings. <<http://www.acm.org/usacm/SSSCA-letter.html>>. Visited 29 October 2001.
- [82] Simon Singh. *The Code Book: The Secret History of Codes and Codebreaking*. Fourth Estate, London, U.K., 1999.
- [83] Red Hat Software. Legislative alert: SSSCA—Security Systems Standards and Certification Act. <<http://www.redhat.com/opensourcenow/article2.html>>. Visited 30 October 2001.
- [84] Security Systems Standards and Certification Act. <<http://cryptome.org/sszca.htm>>. Visited 30 October 2001.
- [85] Richard Stallman. The GNU manifesto. <<http://www.gnu.org/gnu/manifesto.html>>. Visited 30 October 2001.
- [86] Richard Stallman. Why software should be free. <<http://www.gnu.org/philosophy/shouldbefree.html>>. Visited 30 October 2001.
- [87] Richard Stallman. Why software should not have owners. <<http://www.gnu.org/philosophy/why-free.html>>. Visited 30 October 2001.
- [88] Richard M. Stallman. Why GNU/Linux? <<http://www.gnu.org/gnu/why-gnu-linux.html>>. Visited 30 October 2001.
- [89] Mark Stefik. Trusted systems. *Scientific American*, 276(3):78–81, March 1997.
- [90] Neal Stephenson. *In The Beginning... Was The Command Line*. Avon Books, New York, N.Y., U.S.A., November 1999.

- [91] Michael Stroud. Napster wants license to license. <<http://www.wired.com/news/mp3/0,1285,47977,00.html>>. Visited 1 November 2001.
- [92] Anita Stuhmcke. *Legal Referencing*. Butterworths, Sydney, N.S.W., Australia, second edition, 2000.
- [93] Patrick Thibodeau. UCITA goes back to the drawing board. <[http://www.computerworld.com/storyba/0,4125,NAV47\\_STO62803,00.html](http://www.computerworld.com/storyba/0,4125,NAV47_STO62803,00.html)>. Visited 31 October 2001.
- [94] Lee Tien. Publishing software as a speech act. *Berkeley Technology Law Journal*, 15:629–712, 2000.
- [95] David S. Touretzky. Free speech rights for programmers. *Communications of the ACM*, 44(8):23–25, August 2001.
- [96] Fred von Lohmann. Hackers: The new champions of the first amendment. *The California Lawyer*, June 2001.
- [97] Fred von Lohmann. IAAL: Peer-to-peer file sharing and copyright law after Napster. <[http://www.eff.org/Intellectual\\_property/P2P/Napster/20010227\\_p2p\\_copyr%ight\\_white\\_paper.html](http://www.eff.org/Intellectual_property/P2P/Napster/20010227_p2p_copyr%ight_white_paper.html)>, 2001. Visited 1 November 2001.
- [98] George Voyatzis and Ioannis Pitas. The use of watermarks in the protection of digital multimedia products. *Proceedings of the IEEE*, 87(7):1197–1207, July 1999.
- [99] Whatis.com. peer-to-peer. <[http://searchnetworking.techtarget.com/sDefinition/0,,sid7\\_gci212769,00%.html](http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212769,00%.html)>. Visited 1 November 2001.
- [100] Raymond B. Wolfgang, Christine I. Podilchuk, and Edward J. Delp. Perceptual watermarks for digital images and video. *Proceedings of the IEEE*, 87(7):1108–1126, July 1999.
- [101] Alfred C. Yen. Internet service provider liability for subscriber copyright infringement, enterprise liability and the First Amendment. *Georgetown Law Journal*, 88:1833–1893, 2000.
- [102] Junko Yoshida and George Leopold. Copy protection bill divides industry, Hollywood. <<http://www.eetimes.com/story/OEG20010928S0110>>. Visited 29 October 2001.