

**DIGITISING COPYRIGHT LAW — AN AUSTRALIAN PERSPECTIVE**

LEIF GAMERTSFELDER<sup>1</sup>

ABSTRACT

[13] The Commonwealth Parliament recently passed the *Copyright Amendment (Digital Agenda) Act 2000* (Cth). That Act will usher in a number of significant amendments to the Australian *Copyright Act 1968*. These amendments go some way to aligning Australian copyright law with Australia's obligations prescribed under the World Intellectual Property Organisation (WIPO) Copyright Treaty and WIPO Performances and Phonograms Treaty. The purpose of this article is to explain the possible impact of the amendments concerning technological protection measures, circumvention devices and electronic rights management information.

**Introduction**

Under the World Intellectual Property Organisation (WIPO) Copyright Treaty and WIPO Performances and Phonograms Treaty (WIPO treaties), Australia is obliged to amend the *Copyright Act 1968* in order to address the threats posed to digital intellectual property by rapid developments in technology.

In accordance with its obligations under the WIPO treaties, the Commonwealth Parliament passed the *Copyright Amendment (Digital Agenda) Act 2000* (Cth) (Digital Agenda Act). The provisions are intended to address concerns of copyright owners in a digital age. It is certainly arguable that the amendments do adequately address some of the challenges that copyright owners face when making their works available in digital form. However, some of the amendments do give rise to a number of anomalies which might have to be cured if those amendments are to have any longevity. One of the purposes of this article is to point out some of those anomalies.

The main focus of this article will be the amendments relating to technological protection measures, circumvention devices and electronic rights management

---

<sup>1</sup> LLB (Hons) BA Griffith University; Solicitor, Deacons Lawyers, Sydney, Australia <leif.gamertsfelder@deaconslaw.com.au>. Thanks to Justice Michael Kirby of the High Court of Australia for motivating me to write this article. Thanks also to Bo Kim (Deacons) for useful comments on earlier drafts of this article and to Alison Stonham (Deacons) for her research assistance.

information.<sup>2</sup> The recent amendments cover far more ground than these areas, but the challenges facing Parliament in delivering effective legislation in the digital age are clearly demonstrated by the subject matter of this article.<sup>3</sup>

#### **[14] New rights available under the Digital Agenda Act**

As mentioned above, the focus of this article is on the possible application of the amendments concerning the technological protection measures, circumvention devices and electronic rights management information. Also, this article focuses primarily on the civil causes of actions provided for in the Digital Agenda Act, not the corresponding criminal provisions. However, many of the issues discussed in this paper will be equally applicable in the context of any criminal proceedings brought under the Digital Agenda Act amendments to the *Copyright Act 1968* (Cth).

The Digital Agenda Act provides greater protection for digital works by amending the *Copyright Act 1968* (Copyright Act). For convenience all further references in this article will be to the *Copyright Act* as amended by the Digital Agenda Act.<sup>4</sup>

#### ***Technological protection measures***

To take advantage of one of the new rights in the *Copyright Act*, a person must first apply a *technological protection measure* to that person's work or other subject matter.<sup>5</sup>

The *Copyright Act* defines a 'technological protection measure' as:

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.<sup>6</sup>

---

<sup>2</sup> The focus will be on the civil provisions and not the criminal provisions enacted by the *Copyright Amendment (Digital Agenda) Act 2000*.

<sup>3</sup> Other important amendments include those to do with dealings in decoders (Pt VAA) and re-transmission of free-to-air broadcasts (Pt VC).

<sup>4</sup> The provisions discussed in this article will commence operation on 4 March 2001.

Basically, paragraph (a) describes any type of device (such as encryption) that ordinarily prevents access to a work unless the owner supplies a key or code which the user enters into a computer to get access to the work. In relation to paragraph (b), a copy control mechanism is any device that ordinarily prevents or inhibits a person copying a digital product.

In practice, many copyright owners and other vendors of digital products already put encrypted versions of their products on the internet and then require consumers to pay them a fee prior to the vendor releasing a unique key or code to the consumer, which will then enable that consumer to gain access to the digital product or work.

Unfortunately, many processes used by vendors of digital products are capable of being circumvented. In order to deter this activity, the *Copyright Act* now provides for civil and criminal penalties if a person engages in certain conduct relating to *circumvention devices*. Section 10(1) defines a *circumvention device* as:

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.<sup>7</sup>

[15] One example of a circumvention device would be a computer program coded by a hacker or cracker<sup>8</sup> who designed the program to allow unauthorised access to a work protected by encryption. However, the term device is not exhaustively defined in the *Copyright Act*. Apart from computer programs (which are specifically referred to in the *Copyright Act*, many other objects may fall within this definition. The *Macquarie Dictionary* defines 'device' as (among other things) '1) an invention or contrivance ... 2) a plan for effecting a purpose'.

Accordingly, any invention, plan or contrivance may fall within the definition of circumvention device. This means that books, articles, teaching notes and the like could

---

<sup>5</sup> Generally, the discussion in this article assumes the existence of a 'work' or other subject matter for the purposes of the *Copyright Act 1968* (Cth).

<sup>6</sup> See *Copyright Act* s 10(1)

<sup>7</sup> The term 'circumvention service' has a corresponding meaning: see *Copyright Act* s 10(1).

<sup>8</sup> For a discussion about the distinction between a 'hacker' and a 'cracker' see D Denning, *Information Warfare and Security* (1999) 44–5.

all fall within the scope of the definition.<sup>9</sup> This may be true even if the relevant text was student text designed for computer science course which assisted students to learn the finer points of cryptography or cryptanalysis. As a circumvention device merely needs to 'facilitate' circumvention this interpretation of the statute is certainly open.

Ultimately, though, the key issue will be whether an alleged device has a 'commercially significant purpose or use'. Material supplied in the course of education may satisfy this requirement because education arguably falls within the scope of the term 'commercial purpose'. However, this leads into further problems. If the provision of education is enough to take an act outside the scope of the anti-circumvention measures, then it is arguable that the commercial sale of a book on hacking technology would also fall outside the scope of those provisions. Indeed, as long as one can point to an independent commercial purpose, a device will not fall within the scope of the *Copyright Act*.

For example, if one were to discover that a bug in a browser could be exploited so as to allow a user to circumvent a technological protection measure on a copyright owner's website, the use of the browser to circumvent the technological protection measure would not be unlawful because browsers have an independent commercial purpose. This result will follow because the use of technological protection measures is not unlawful under the *Copyright Act*. Users exploiting such bugs could then arguably view works on a copyright owner's website or listen to streamed music files because if such acts fell within the terms of the temporary reproduction right contained in s 43A of the *Copyright Act*. Section 43A(1) provides that:

The copyright in a work, or an adaptation of a work, is not infringed by making a temporary reproduction of the work or adaptation as part of the technical process of making or receiving a communication.

The process of viewing a JPEG image or listening to streamed music arguably falls within the scope of the term communication in that both processes rely on making or receiving data communications over the internet. Assuming that this logic is accepted

---

<sup>9</sup> Even if such material did not fall within the scope of the term 'circumvention device' it may fall within the scope of the term 'circumvention service'.

by a court, an infringement action may not lie against a person using a browser in the manner outlined immediately above. However, s 43A(2) adds another layer of complexity at this point. Section 43A(2) provides that s 43A(1) does not apply:

in relation to the making of a temporary reproduction of a work, or an adaptation of a work, as part of the technical process of making a communication if the making of the communication is an infringement of copyright.

Importantly, the exception in s 43A(2) does not apply to refer to 'receiving' communications. Accordingly, meaning has to be given to the words that Parliament chose to use in s 43A(1) on one hand and s 43A(2) on the other. As acts such as viewing JPEG images online or listening to streamed music files both involve [16] the reproduction of temporary copies of works during the *receipt* phase of World Wide Web communications it is arguable that s 43A(2) does not apply in the scenario outlined above because no temporary reproduction is made during the *receipt* phase, not the propagation or *making* phase of the communication cycle which is generally just a request for information.

This approach to interpreting s 43A(2) would not deprive that provision of any meaning. Section 43A(2) would be triggered in a wide range of instances. For instance, if an infringing copy of a JPEG image was attached to an email message, such a communication would be the *making* of a communication within the terms of s 43A(2).

The *Copyright Act* does not prohibit the actual *use* of circumvention devices or services. It prohibits the manufacture and general supply of such devices. Parliament adopted this approach because it was of the view that it would be more effective for owners of copyright to be able to seek remedies against those who manufactured or supplied circumvention devices rather than against individual users of such devices.<sup>10</sup>

Section 116A of the *Copyright Act* is the substantive provision which actually prohibits certain dealings in circumvention devices. There are three main elements which must be satisfied before an action under s 116A of the *Copyright Act* may proceed. The first element provides that a work or other subject matter must be protected by a

technological protection device<sup>11</sup>. The second element will be satisfied where a person, in relation to work or other subject matter so protected, does one of the following acts without the copyright owner's or the exclusive licensee's authority:

- makes a circumvention device capable of circumventing or facilitating the circumvention of the technological protection mechanism protecting the work or other subject matter;<sup>12</sup>
- sells, lets for hire, offers for sale, promotes, advertises or markets such a circumvention device;<sup>13</sup>
- distributes such a circumvention device in trade or for any other purpose that will prejudicially affect the owner of the copyright;<sup>14</sup>
- exhibits such a circumvention device in public by way of trade;<sup>15</sup>
- imports such a circumvention device for a trade-related purpose;<sup>16</sup>
- makes such a circumvention device available online in a manner that prejudicially affects the owner of the copyright; or<sup>17</sup>
- provides, or by way of trade, promotes, advertises or markets a circumvention service capable of circumventing or facilitating the circumvention of the technological protection device.<sup>18</sup>

As noted above, the aim of the *Copyright Act* is not to prohibit the actual use of circumvention devices but rather commercial dealings in such devices.<sup>19</sup> In fact, it will not be a breach of the amendments to [17] the *Copyright Act* if a person imports a circumvention device for *personal* use; only trade-related purposes are prohibited.<sup>20</sup> However, this may prompt those that deal with circumvention devices to set up

---

<sup>10</sup> See *Exposure Draft and Commentary — Copyright Amendment (Digital Agenda) Bill 1999*, 24.

<sup>11</sup> See *Copyright Act* s 116A(1)(a).

<sup>12</sup> See *Copyright Act* s 116A(1)(b)(i).

<sup>13</sup> See *Copyright Act* s 116A(1)(b)(ii).

<sup>14</sup> See *Copyright Act* s 116A(1)(b)(iii).

<sup>15</sup> See *Copyright Act* s 116A(1)(b)(iv).

<sup>16</sup> See *Copyright Act* s 116A(1)(b)(v).

<sup>17</sup> See *Copyright Act* s 116A(1)(b)(vi).

<sup>18</sup> See *Copyright Act* s 116A(1)(b)(vii).

<sup>19</sup> This approach contrasts with the approach in the US. Under US copyright law, the 'act of circumventing a technological protection measure put in place by a copyright owner to control access to a copyrighted work' is prohibited [see s 1201(a)(1), *Digital Millennium Copyright Act* (US)]. In addition to prohibiting commercial dealings in circumvention devices, US law prohibits the making available of such devices whether such availability is provided for the purposes of trade [see s 1201(a)(2), *Digital Millennium Copyright Act* (US)]. The Australian approach is therefore much narrower than the US approach.

websites offshore and lawfully service a market in circumvention devices in Australia by encouraging individuals to import, for personal use, such devices from the offshore website.<sup>21</sup> In this scenario, it is strongly arguable that there would be no dealing with devices in Australia.<sup>22</sup>

Even if the first two elements of s 116A are satisfied, however, liability under the *Copyright Act* for a breach of the provisions relating to technological protection measures will only arise if the third element is satisfied and no exemptions apply. The third element of s 116A(1) provides that a person may be liable under the technological protection measure provisions if:

the person knew, or ought reasonably to have known, that the device or service would be used to circumvent, or facilitate the circumvention of, the technological protection measure.<sup>23</sup>

Importantly, the *Copyright Act* reverses the onus of proof in relation to the third element.<sup>24</sup> Where an action is brought under s 116A, it *must* be presumed that:

the defendant knew, or ought reasonably to have known, that the circumvention device or service to which the action relates would be used for a purpose referred to in ... [s 116A(1)(c)] unless the defendant proves otherwise.

In placing the onus of proof on the defendant, Parliament appears to have assumed that it would be much easier for the defendant to rebut the presumption than for copyright owners to satisfy the onus of proof if they had the burden of doing so.<sup>25</sup>

---

<sup>20</sup> This does not mean that other copyright or even contractual rights will not be infringed by such conduct, though.

<sup>21</sup> This scenario assumes that no advertising or promotion of the scheme actually occurs in Australia per se. The issue of whether a website accessible by Australians can be considered advertising in Australia will be put to one side for the purposes of this article. However, even if that question was answered in the affirmative, the issue of effective cross-border remedies against the advertiser or promoter would arise.

<sup>22</sup> Copyright owners may however attempt to enforce the provisions relating to making devices available online or the provisions relating to the promotion of devices, but this will not be easy as cross border litigation issues such as the enforcement of foreign judgments become a major obstacle.

<sup>23</sup> See *Copyright Act* s 116A(1)(c).

<sup>24</sup> See *Copyright Act* s 116A(6).

<sup>25</sup> This approach is not unknown to Australian copyright lawyers. *Copyright Act* s 130A (which applies in relation to the importation of sound recordings) contains a similar provision.

If the three elements discussed above are satisfied, then a copyright owner or exclusive licensee may successfully bring an action against a defendant for infringement<sup>26</sup> unless an exemption applies.

### *Exemptions*

Two important exemptions apply. First, proceedings cannot be brought in relation to anything done for the purposes of law enforcement or national security.<sup>27</sup> Secondly, and more importantly, s 116A will not apply in relation to:

the supply of a circumvention device or circumvention service to a person for use for a permitted purpose if:

- (a) the person is a qualified person; and
- (b) the person gives the supplier before, or at the time of, the supply a declaration signed by the person: [18]
  - i. stating the name and address of the person; and
  - ii. stating the basis on which the person is a qualified person; and
  - iii. stating the name and address of the supplier of the circumvention device or circumvention service; and
  - iv. stating that the device or service is to be used only for a permitted purpose by a qualified person; and
  - v. identifying the permitted purpose by reference to one or more of sections 47D, 47E, 47F, 48A, 49, 50, 51A and 183 and Part VB; and
  - vi. stating that a work or other subject matter in relation to which the person proposes to use the device or service for a permitted purpose is not readily available to the person in a form that is not protected by a technological protection measure.<sup>28</sup>

The permitted purposes referred to in s 116A(3) include: reverse engineering, error correction, security testing, library copying for users and copying by the Crown.<sup>29</sup>

---

<sup>26</sup> See *Copyright Act* s 116A(5).

<sup>27</sup> See *Copyright Act* s 116A(2).

<sup>28</sup> See *Copyright Act* s 116A(3).

<sup>29</sup> See ss 47D(1)(a) [reverse engineering]; 47E(1)(a) [error correction]; 47F(1)(a) [security testing]; 48A [copying by Parliamentary libraries for members of Parliament]; 49 [copying by libraries and archives for users]; 50 [copying by libraries or archives for other libraries or archives]; 51A [copying of works for preservation and other purposes]; 183 [a person authorised by the Commonwealth or a State for certain purposes]; or Pt VB [a person authorised for certain purposes by a body administering an institution within the meaning of that term under Pt VB].

The matter addressed in s 116A(3)(b)(vi) in relation to a work or other subject matter not being 'readily available' is an important one. Section 116A(4) provides that a work or other subject matter will not be readily available if it is not available in a form that allows a person to exercise a right under s 47D, 47E, 47F, 48A, 49, 50, 51A or 183 or Pt VB. Defendants may find this a difficult condition to satisfy.

Take computer software for example. Assume an organisation runs a certain computer program which has a technological protection measure applied to it. If that program exhibits a defect when executing certain commands, the organisation may be able to correct that defect by exercising its rights under s 47E of the *Copyright Act* if the requirements of that provision, which in themselves are quite onerous, are satisfied. However, if the same program is available on the internet or in stores in an unprotected form, it is arguable that the computer program is 'readily available' for the purposes of s 116A(4). For example, a computer program may have a technological protection measure applied to it in the Australian market, but be available in unprotected form in another country because of a ban on encryption technologies in that country. In these circumstances, organisations may be prohibited from exercising their rights under s 47E.

It is difficult to know how much searching one should advise an organisation to conduct in determining whether a program is 'readily available'. If a program is available online somewhere on the internet it is arguably 'readily available'. If this assertion is correct, the *Copyright Act* appears to require organisations to purchase the 'unprotected' version of the program and *then* exercise its rights under s 47E. If this proposition is true, the law runs the risk of producing some perverse outcomes. Further, how much cost will need to be incurred before something is no longer 'readily available'? If cost is a criterion arbitrary results may follow. Wealthy companies may be forced to buy duplicative programs while less wealthy companies will not be required to do so. It appears that the only way to ensure that consistent outcomes are achieved is to disregard subjective factors and assess the issue from an objective standpoint.

Taken separately, the requirements in ss 47D, 47E and 47F on the one hand, and the requirements under s 116A(3) and 116A(4) are arguably reasonable in light of the ease with which digital piracy can be performed. However, the net effect of these

requirements appears to be that they effectively render the rights users were granted under the *Copyright Amendment (Computer Programs) Act 2000* illusory.<sup>30</sup> This is because compliance with these requirements is extremely difficult in many cases. It is not easy to comprehend [19] why Parliament has superimposed onerous obligations on top of the taxing pre-conditions to the valid exercise of rights under ss 47D, 47E and 47F.

Fortunately, for those exercising rights under ss 48A, 49, 50, 51A or 183 or Pt VB, their rights retain some substance. Indeed, this appears to be because Parliament has drafted ss 116A(3) and 116A(4) with traditional copyright matter in mind, such as photographs and text as opposed to computer programs. In fact, the 'readily available' requirement makes perfect sense when applied to traditional copyright material such as books and photographs. Conversely, it makes little sense when applied to computer programs, especially in light of the onerous conditions that must be satisfied under ss 47D, 47E and 47F of the *Copyright Act*.

Computer program users are not the only right holders that witness the wasting of their existing rights under the *Copyright Act*. The fair dealing rights that copyright users enjoy will not apply in relation to works which have technological protection measures applied to them. The fair dealing rights that are affected are:

- fair dealing for purpose of research or study;<sup>31</sup>
- fair dealing for purpose of criticism or review;<sup>32</sup>
- fair dealing for purpose of reporting news;<sup>33</sup> and
- reproduction for purpose of judicial proceedings or professional advice.<sup>34</sup>

Once a copyright owner applies a technological protection measure to a digital work, these rights are effectively lost in cyberspace. While copyright users will lawfully be able to *use* circumvention devices under the new regime, their access to these devices will be limited because of the almost blanket prohibition on commercial dealings with such devices. On the other hand, copyright users will still be able to exercise these

---

<sup>30</sup> This Act amended the *Copyright Act* by inserting (among others things) ss 47D, 47E and 47F.

<sup>31</sup> See *Copyright Act* s 40.

<sup>32</sup> See *Copyright Act* s 41.

<sup>33</sup> See *Copyright Act* s 42.

<sup>34</sup> See *Copyright Act* s 43.

rights in the analogue world. However, this may be cold comfort in an age where the predominate means of distribution for works will be the internet.

Another important feature of the second exemption is that it is limited to the *supply* of circumvention devices. The word 'supply' is defined to mean:

- (a) in relation to a circumvention device — sell the device, let it for hire, distribute it or make it available online; and
- (b) in relation to a circumvention service — provide the service.<sup>35</sup>

Importantly, organisations that are in a position to 'supply' circumvention devices or services to copyright users will not be able to exhibit, advertise, promote or market this fact. This is because these activities, in relation to circumvention devices or services do not fall within the definition of the term 'supply'. This begs the question: How do organisations communicate the availability of circumvention devices and services to copyright users? It appears that they may be prohibited from doing so because the words 'exhibit', 'advertise', 'promote' and 'market' are words of wide import. If copyright users are not made aware of the availability of circumvention devices or services, they will not be able to exercise the fragile rights that the *Copyright Act* confers on them. This surely could not be Parliament's intention in drafting s 116A, but it appears to be the effect.<sup>36</sup>

[20] For the purposes of the second exemption mentioned above, a 'qualified person' is one who is authorised to do certain acts in relation to copyright material under various

---

<sup>35</sup> See *Copyright Act* s 116A(8).

<sup>36</sup> Universities should note that under the new laws, if a program is protected by a technological protection measure it will be unlawful to circumvent it for general research purposes. All activities would have to strictly fall within the scope of one of the exemptions. Also, it would take some creative minds to overcome the requirement to produce an interoperable program if the rights in s 47D were to be exercised. Under that section the person conducting the reverse engineering must be doing so to make an interoperable program on by or on *behalf of* the owner of the original program. This means that the university will need to be making interoperable programs or that its students will need to purchase a copy of the program that is to be reverse engineered. Reverse engineering conducted merely to study underlying ideas in a program will be prohibited. It is also important to note that program-to-program interoperability is the only exemption provided for under s 47D of the *Copyright Act*. Data-to-program interoperability is not covered by the Act. For example, the intended creation of an emulator which allowed a movie file or music file to run on a platform other than the original platform would not fall within the scope of s 47D (and hence s 116A(3)) as the emulator (the 'new program' for the purposes of s 47D(1)(b)) would not be a program designed 'to connect to and be used together with, or otherwise to interoperate with, the original program or any other program'. It would be a program designed to interoperate with a data file.

provisions in the *Copyright Act*.<sup>37</sup> Unlike many of its sister provisions, this requirement does not give rise to any material concerns.

The requirement for a 'signed' declaration under the second exemption, raises some interesting online authentication issues. While traditional analogue signatures on paper will comply with this requirement, as more and more communications are conducted over the internet, virtual signatures will only be acceptable if they comply with the requirements of s 10 of the *Electronic Transactions Act 1999* (Cth).<sup>38</sup> In the near future it is arguable that only digital signatures used under a robust public key infrastructure will satisfy these requirements.<sup>39</sup> Therefore the overheads associated with compliance with this exemption may be quite high. This could have a particularly adverse affect on any electronic security organisation attempting to supply circumvention devices to its clients in order for those clients to exercise their rights under s 47F of the *Copyright Act*.

For example, if a certain security vulnerability is discovered in a popular computer program and an immediate patch or fix is required to be applied to that program, e-security firms normally post patches or fixes on their websites, which clients may then download. Even where advanced technology is used this can put a tremendous strain on bandwidth when anti-virus solutions or other fixes are urgently required by clients.<sup>40</sup> This can lead to extremely slow download times or aborted attempts to download. The longer it takes for the user to successfully download the patch or fix the wider the window of opportunity for a hacker to exploit a vulnerability in the user's

---

<sup>37</sup> See ss 47D(1)(a) (reverse engineering); 47E(1)(a) (error correction); 47F(1)(a) (security testing); 48A (copying by Parliamentary libraries for members of Parliament); 49 (copying by libraries and archives for users); 50 (copying by libraries or archives for other libraries or archives); 51A (copying of works for preservation and other purposes); 183 (a person authorised by the Commonwealth or a State for certain purposes); or Pt VB (a person authorised for certain purposes by a body administering an institution within the meaning of that term under Pt VB).

<sup>38</sup> This Act and not the mirror State Acts will apply as the declaration is to be given for the purposes of a law of the Commonwealth: see *Electronic Transactions Act 1999* s 10(1).

<sup>39</sup> For more information on digital signatures and public key infrastructure see For an overview of digital signatures and public key infrastructure see: B Schneier, *Secrets and Lies: Digital Security in a Networked World* (2000) 'Chapter 15 — Certificates and Credentials'; A McCullaugh, 'Chapter 11 — Legal aspects of electronic contracts and digital signatures' in A Fitzgerald, B Fitzgerald, C Cifuentes and P Cook, *Going Digital: Legal issues for e-commerce, software and the internet* (2000); Denning, above n 8, 331–7; and L Stein, *Web Security: a step-by-step reference guide* (1998) 'Chapter 2 — Basic Cryptography'.

<sup>40</sup> For example, when the Melissa or ILOVEYOU viruses infected information systems around the world.

information systems. This situation could be made worse by a significant magnitude under the amendments to the *Copyright Act*.

[21] Where a patch or fix needs to be coupled with a circumvention device or service for it to be implemented, copyright users must first send an e-security firm which legitimately supplies circumvention devices a signed declaration under s 116A(3). If a digital signature is required, suppliers will need to ensure that their information systems are capable of authenticating their clients' digital signatures in real time in urgent situations. Suppliers will also need to ensure that the current certificate revocation list is interrogated or an online certificate status protocol<sup>41</sup> is used. This is normal practice under PKI and will invariably be a contractual obligation.

Aside from the overheads for storing and archiving digital certificates that the *Copyright Act* will foist on security providers, the Act will also put an incredible burden on the servers of the supplier of the patch or fix. Consequently, in situations where urgent patches or fixes are required — such as when the Melissa and ILOVEYOU viruses struck — and a technological protection measure needs to be circumvented a difficult task (that is, obtaining an urgent patch or fix) will be made more difficult under the amendments to the *Copyright Act*.

In practice, not only may the information systems of a legitimate supplier of circumvention devices have to cope with PKI overheads under the second exemption, suppliers will have to ensure that they retain copies of all digitally signed declarations for at least the six year statute of limitation period that applies to civil actions under the *Copyright Act*.<sup>42</sup> This will involve ensuring backward compatibility of any information systems that it uses in the future to ensure that those systems can read historical declarations. More importantly, where digital signatures are used, the supplier will need to ensure that it can verify those signatures at both the time a signed declaration is provided and at anytime that civil proceedings might be brought against it — that is, for at least the six year limitation period. These are not insignificant considerations.

---

<sup>41</sup> As is used in the Identrus public key infrastructure.

<sup>42</sup> See *Copyright Act* s 134(2).

Another activity that the new provisions would appear ill-equipped to prevent is the manipulation of regional coding in DVDs. DVD players contain a mechanism which can be manipulated so that the vendors of DVD works can ensure that only DVDs purchased in a certain region can be played on DVD players purchased in the same region. It is not uncommon for retailers of DVD players to reset the access controls in those players. At first blush this may appear to fall within the ambit of the circumvention provisions. However, upon close analysis of the provisions this does not appear to be the case.

Under the *Copyright Act* a 'technological protection measure' must in the ordinary course of its operation 'prevent or inhibit the infringement of copyright'. In the case of legitimate DVDs purchased by the owner of DVD player, the region coding system may never 'prevent or inhibit the infringement of copyright'.<sup>43</sup> This is because individuals that purchase the DVDs do not enter into a licence agreement with the vendors of DVDs stipulating that the DVDs can only be played on a DVD player containing a certain regional code. In fact, in most cases it appears that no effective licence is entered into. Accordingly, if a user is never going to be in breach of a contractual provision which limits his or her right to use DVD on a DVD player with a specific regional code, it follows then that a retailer manipulating the regional code in a DVD player will never be providing a circumvention service because the regional code is not something that prevents or inhibits the infringement of copyright.

One possible counter argument is that the regional coding is designed to prevent or inhibit the supply of pirated DVDs from one region, say South East Asia, being played on DVD players purchased in another region such as Australia. This argument assumes that the issue of possible infringement is considered from a global, objective position; not from the perspective of the individual user. While this argument holds some attraction, it is fragile in light of the fact that the predominant effect of a retailer resetting the regional coding would be to assist the owners of legitimate DVDs (irrespective of the region in which [22] they purchased these DVDs) play them on their DVD players. Such a procedure is not to assist the purchases of DVD players to infringe copyright in DVDs. In the absence of a contractual term preventing DVD

---

<sup>43</sup> See *Copyright Act* s 10(1).

owners from playing DVDs on a DVD player with a specific regional coding, this reasoning should prevail.

One activity that the circumvention provisions might prohibit yet perhaps should be exempted is the supply of circumvention devices or services in respect of malfunctioning or obsolete technological protection measures. Such an exemption is available under the US *Copyright Act 1976*. On 27 October 2000, the Librarian of Congress made a determination under the US *Copyright Act* which provides that literary works (including computer programs and databases) which are protected by access control mechanisms that fail to permit access because of malfunction, damage or obsolescence will fall outside the scope of the circumvention provisions under US law.<sup>44</sup> This issue has yet to receive any legislative attention in Australia.

In the absence of any legislative action, it is arguable that the supply of circumvention devices or services to allow copyright users to circumvent malfunctioning or obsolete technological protection measures applied to computer programs will be unlawful. This would appear to be a very harsh outcome given the high likelihood of a technological protection measure failing.

#### *Malfunctioning or obsolete protection measures*

Where a malfunctioning or faulty technological protection measure is a computer program within the meaning of that term in the *Copyright Act*, parties may be able to exercise the error correction rights in s 47E without having to comply with the circumvention provisions. This may be possible because if error correction is performed in relation to a malfunctioning technological protection measure, there is no element of circumvention involved. The reverse engineering is being performed on the technological protection measure itself; there is no element of circumvention within the scope of the *Copyright Act* for two reasons. First, there will probably not be any technological protection measure applied to the faulty technological protection measure. Therefore, the *Copyright Act* will not apply. Secondly, circumvention in these cases will not involve a technological protection measure being bypassed within the

---

<sup>44</sup> See *Recommendation of the Register of Copyrights and Determination of the Librarian of Congress*, 65 FR 64555 at 64564, effective 28 October 2000, <<http://www.loc.gov/copyright/1201/anticirc.html>>.

ordinary sense of that word. A person will obtain access to the measure itself, not circumvent or bypass it.

Despite the possible s 47E providing some assistance in this area, it would be preferable for Parliament to consider an exemption along the lines of those made by the Librarian of Congress in late 2000. First, not all technological protection measures will be computer programs. The rights in s 47E are only available in relation to the reverse engineering of computer programs. Secondly, the exercise of the rights under s 47E are dependant on some strict requirements being met. If a vendors supply faulty protection measures to the market, arguably users should be able to exercise self-help remedies without having to meet these requirements.

By providing narrow exemptions to the prohibitions on dealings with circumvention devices the apparent aim of the legislature is to extend the scope of copyright for digital works and other subject matter as opposed to the protection afforded to analogue works and subject matter. This point is brought into sharp relief when one considers that once a technological protection measure is applied to a work or other subject matter, a party will not be able to exercise any fair dealing right.<sup>45</sup> Accordingly, the balance is tipped strongly in favour of copyright owners in the digital age. The justification for this change of position appears to be due to the ease with which copyright in digital works and other subject matter can be infringed.

In order to better understand the impact of the recent amendments to the *Copyright Act* it is instructive to examine US case law which has examined these issues under legislation containing similar provisions.

### [23] **Case law**

At the date of writing there have been no cases under s 116A.<sup>46</sup> However, there has been a US case which has considered similar provisions contained in the US *Digital Millennium Copyright Act (DMCA)*. This case provides some useful insights into how s 116A may be interpreted by Australian courts.

---

<sup>45</sup> The fair dealing rights are set out in *Copyright Act* ss 40, 41, 42 and 43.

<sup>46</sup> The circumvention provisions come into force on 4 March 2001.

In *Universal City Studios Inc v Reimerdes*<sup>47</sup> (the DeCSS case) the court granted an injunction preventing the defendants from making the DeCSS program available to the public or otherwise dealing with the DeCSS program, including linking to sites that hosted the DeCSS program. The DeCSS program is a device which enabled users to break the encryption used to protect movies burnt onto DVDs.

In the DeCSS case the defendants unsuccessfully argued that the prohibitions in the DMCA did not apply as their conduct fell within the compass of exemptions contained in the DMCA. Many of these exemptions have counterparts in the *Copyright Act* and it is therefore interesting to see how the defendants' arguments on these points were dealt with by the US court in this case.

### ***'Effective' Circumvention Devices***

First, the DMCA prohibits certain dealings in devices that circumvent 'effective' technological protection measures. The defendants argued that because the DeCSS program was able to circumvent the CSS protection measure, it must by definition be *ineffective*.<sup>48</sup> They therefore argued that their conduct did not fall within the scope of the DMCA. The court bluntly rejected this argument. The Court held that:

As CSS, in the ordinary course of its operation — that is, when DeCSS or some other decryption program is not employed — 'actually works' to prevent access to the protected work, it 'effectively controls access' within the contemplation of the statute.

Finally, the interpretation of the phrase 'effectively controls access' offered by the defendants at trial — viz, that the use of the word 'effectively' means that the statute protects only successful or efficacious technological means of controlling access — would gut the statute if it were adopted. If a technological means of access control is circumvented, it is, in common parlance, ineffective. Yet defendants' construction, if adopted, would limit the application of the statute to access control measures that thwart circumvention, but withhold protection for those measures that can be circumvented. In other words, defendants would have the Court construe the statute to

---

<sup>47</sup> Unreported, 00 Civ 0277 (LAK), US District Ct, Sth District NY, 17 August 2000. A less celebrated case that has examined these issues is *RealNetworks Inc v Streambox Inc No 2 99CV 02070*, 2000 WL 127311 (WD Wash 18 January 2000).

<sup>48</sup> Unreported, 00 Civ 0277 (LAK), US District Ct, Sth District NY, 17 August 2000, 32.

offer protection where none is needed but to withhold protection precisely where protection is essential. The Court declines to do so.<sup>49</sup>

An Australian court could be faced with the same argument in any case brought under s 116A because under the *Copyright Act* a circumvention device and a circumvention service are ones that have:

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 [emphasis added].

It is difficult to understand why the Australian Parliament persisted with the use of the word 'effective' in this context as it does nothing to ensure certainty in the application of s 116A yet creates interpretative fissures in the foundation of that provision. However, any apparent structural weakness [24] caused by the use of the word 'effective' will hopefully be overcome by a court following the same logic adopted by the court in the DeCSS case.

#### ***'Sole Purpose' requirement***

Second, the defendants argued that 'sole purpose' of the DeCSS program was not to infringe the plaintiff's rights but to create a DVD player for Linux.<sup>50</sup> The Court considered this argument had no merit as it misinterpreted the thrust of the DMCA. That Act prohibits commercial dealings in circumvention devices. It did not matter that the defendants may have been attempting to facilitate the infringement of other forms of copyright under US law. The Court held that the inescapable facts were that:

- CSS was a technology that effectively controlled access to DVDs;
- the sole purpose of DeCSS was to circumvent CSS; and
- the defendants provided access to the DeCSS program online.<sup>51</sup>

Accordingly, the defendants' conduct was in breach of the DMCA. In light of the definition of 'circumvention device' under the *Copyright Act* and the prohibition

---

<sup>49</sup> Ibid 33–4.

<sup>50</sup> Ibid 35.

<sup>51</sup> Ibid 35–6.

against making circumvention devices available online,<sup>52</sup> it is suggested that the same conclusion would follow if an Australian court was called on to consider a similar fact scenario.

### ***Reverse engineering***

Third, the defendants attempted to rely on a statutory exemption under the DMCA which permits reverse engineering in certain circumstances.<sup>53</sup> Under US law a person may circumvent access control measures in order to achieve interoperability with another computer program.<sup>54</sup> Also, one may make any information acquired during such procedures 'available to others, if the person ... provides such information *solely* for the purpose of enabling interoperability of an independently created computer program with other programs, and to the extent it does not constitute infringement' (emphasis added).<sup>55</sup> The defendants in the DeCSS case argued that the DeCSS program was necessary to achieve interoperability between computers running the Linux operating system and therefore the reverse engineering exception was satisfied. The court rejected these arguments.

Under US law, information obtained during the reverse engineering process can only lawfully be made available to others by the person that conducted the reverse engineering. The defendants did not perform any reverse engineering in the DeCSS case. Further, the court found that the defendants would have been in no better position even if they had conducted the relevant reverse engineering. The court was of the view that the defendants did not post the information 'solely' to achieve interoperability with Linux (as argued by the defendants) or any other program. According to the court the defendants posted the information so that others could use DeCSS as a means of circumventing the CSS program.<sup>56</sup>

The Australian *Copyright Act* also provides a right to conduct reverse engineering.<sup>57</sup> That right is, however, quite narrow.<sup>58</sup> If a case involving similar facts to the DeCSS

---

<sup>52</sup> See *Copyright Act* s 116A(1)(vi).

<sup>53</sup> Above n 48, 36.

<sup>54</sup> See 17 USC ss 1201(f)(1), (2).

<sup>55</sup> See 17 USC s 1201(f)(3).

<sup>56</sup> Unreported, 00 Civ 0277 (LAK), US District Ct, Sth District NY, 17 August 2000, 35–6.

<sup>57</sup> See *Copyright Act* s 47D.

<sup>58</sup> See *Copyright Act* s 47D.

was to be determined under Australian context, it is likely that the same result would follow.

Under Australian law if a defendant argued that it supplied a circumvention device for the purposes [25] of allowing another party to create an emulator for a Linux operating system, the defendant would have to show that the Linux emulator involved reverse engineering for program-to-program interoperability and not reverse engineering for program-to-data purposes. This requirement is mandated under s 47D of the *Copyright Act* (the exception which gives the exemption in s 116A(3) its force). The relevant provision in s 47D provides that:

the reproduction or adaptation is made for the purpose of obtaining information necessary to enable the owner or licensee to make independently another program (the new program), or an article, to connect to and be used together with, or otherwise to interoperate with, the original program or any other program.<sup>59</sup>

The key requirement in this provision is the need to create a program that interoperates with the 'original program or any other program'. A Linux emulator capable of playing DVD movies would not meet this requirement because the Linux emulator would interoperate with a data file (that is, the DVD movie) and not 'another program'. Accordingly, the recent amendments to the *Copyright Act* provide exceptions to the circumvention devices only in relation to reverse engineering for program-to-program interoperability and not reverse engineering for program-to-data purposes.<sup>60</sup>

### ***Security Testing***

Fourth, the defendants argued that their conduct was permitted under security testing provisions in the DMCA.<sup>61</sup> Under s 1201(j) of the DMCA the security testing exception is limited to:

---

<sup>59</sup> *Copyright Act* s 47D(1)(b).

<sup>60</sup> See also P Samuelson, 'Towards More Sensible Anti-Circumvention Regulations' *Proceedings of the Financial Cryptography 2000 Conference* <<http://www.sims.berkeley.edu/~pam/papers.html>>. One consequence of this situation is that technological protection measures could be used not only to protect content (eg, in DVD movies) but also to reinforce the dominance of a particular operating system or platform: see Fitzgerald, B., 'Intellectual Property Rights in Digital Architecture (including software): The Question of Digital Diversity?' Paper delivered at the IEEE Working Conference on Reverse Engineering 2000, Brisbane, Australia, (Forthcoming as an *Opinion* in [2001] EIPR, 5).

<sup>61</sup> Unreported, 00 Civ 0277 (LAK), US District Ct, Sth District NY, 17 August 2000, 40.

assessing a computer, computer system, or network, solely for the purpose of good faith testing, investigating, or correcting [of a] security flaw or vulnerability, with the authorization of the owner or operator of such computer system or computer network.

The Court held that there was no evidence to suggest that by uploading and hosting the DeCSS program on its website or by providing links to other sites where DeCSS was available the defendants were conducting any security testing in good faith.<sup>62</sup>

Given the same facts, the same result would follow under Australian law for a number of reasons. The most important reason relates to the scope of security testing exemption in the *Copyright Act*. The *Copyright Act* requires that any person making a circumvention device available online must comply with certain requirements. Among other things, the individual or organisation must receive a declaration in the form specified in s 116A(3) of the *Copyright Act*. Further, even if a supplier received such a declaration, only the most reckless or wilfully negligent supplier would rely on such a declaration because the DeCSS program was clearly designed to circumvent devices that prevented access to data files (that is, DVD movies) and not computer programs. As the security testing exemption in the *Copyright Act* only applies to computer programs, it would be difficult for an Australian supplier of DeCSS-type devices to rely in [26] good faith on any declaration received in circumstances where a circumvention device allowed access to a data file as opposed to a program.<sup>63</sup>

### ***Fair use***

Fifth, the defendants relied on the US fair use doctrine, as codified in s 107 of the US *Copyright Act*.<sup>64</sup> The court explained that fair use doctrine:

limits the exclusive rights of a copyright owner by permitting others to make limited use of portions of the copyrighted work, for appropriate purposes free of liability for

---

<sup>62</sup> *Ibid.*

<sup>63</sup> It is interesting to note that the scope of the security testing exemption in the US *Copyright Act* is broader than the Australian provision because the US exemption refers to security testing on 'computers', 'computer systems', and 'computer networks'. Arguably, these words are capable of extending to security testing on data files that are independent of yet are capable of being used on a computer, system or network: Cf s 1201(j), DMCA with *Copyright Act* s 47F.

<sup>64</sup> Above n 61, 40.

copyright infringement ... The doctrine traditionally has facilitated literary and artistic criticism, teaching and scholarship, and other socially useful forms of expression.<sup>65</sup>

The Court then had to decide whether the possibility of 'non-infringing fair use by someone who gains access to a protected copyrighted work through a circumvention technology distributed by the defendants' excused them from liability under s 1201 of the DMCA. The court was of the opinion the words of the statute compelled the court to answer this question in the negative. It was not open to the court to construe the words of the statute to 'accomplish a result that Congress rejected.'<sup>66</sup> Accordingly, under US law, once a technological protection measure is applied to a work, all fair use rights are extinguished.

As discussed above in relation to fair dealing rights under the Australian *Copyright Act*, it is clear that any defendants attempting to rely on those rights to avoid liability in an action claiming a breach of s 116A will be unsuccessful.

### *Other defences*

The defendants in the DeCSS case unsuccessfully attempted to rely on a number of other laws and doctrines which have no direct counterparts under Australian law. They include the right to conduct encryption research<sup>67</sup> and First Amendment (free speech) rights.<sup>68</sup> While these further unsuccessful defences do not provide any direct assistance when interpreting the amendments to the *Copyright Act*, they do demonstrate the extremely robust nature of the rights that have been conferred on copyright owners under the DMCA.

Having failed to mount a successful defence to the claims of the plaintiffs, the defendants were enjoined from dealing in any manner with the DeCSS program, including hosting links to any websites where that program was available.

---

<sup>65</sup> The doctrine has also been extended to cover reverse engineering: see *Sega Enterprises Ltd v Accolade Inc* 977 F 2d 1510 (9th Cir 1992) and *Atari Games Corp v Nintendo of America Inc* 975 F 2d 832 (Fed Cir 1992).

<sup>66</sup> Above n 61, 45.

<sup>67</sup> *Ibid* 38.

### **Striking a new balance**

The DeCSS case provides some excellent insights into how a similar case may be decided under the Australian *Copyright Act*. However, it also confirms that the balance that was previously struck between copyright owners and users has now shifted firmly in favour of copyright owners.

Indeed, the technological protection measure provisions in the *Copyright Act* have shifted the pendulum much further than the preceding discussion indicated. For example, under traditional [27] copyright law infringement will only occur where a person copies a work in its entirety or copies a ‘substantial part’ of a work.<sup>69</sup> Where less than a substantial part of a work is copied, no infringement action will lie.<sup>70</sup> Conversely, under the amended *Copyright Act*, if a technological protection measure is applied to a work, no reproduction — insignificant or otherwise — will be permitted because access to the work is prohibited unless an exemption applies. It is clear from the discussion above in respect of exemptions under the *Copyright Act* that no such exemption applies in relation to the taking of less than a substantial part of a work.

It has also been argued by some US commentators that the application of technological protection measures may limit access to subject matter in relation to which copyright has expired.<sup>71</sup> With respect, this appears to be an erroneous assertion. Under both the Australian *Copyright Act* and the US DMCA technological protection measures only have any force if applied to a ‘work’<sup>72</sup> as defined by statute. By definition, subject matter on which copyright has expired cannot logically be considered a work for the purposes of copyright law. Once copyright expires it is no longer a work for the purposes of copyright law.

---

<sup>68</sup> Ibid 52.

<sup>69</sup> See *Copyright Act* s 14(1).

<sup>70</sup> See for example, *Warwick Films v Eisinger* [1969] Ch 508. For an overview of the concept of ‘substantial part’ see S Ricketson, *The Law of Intellectual Property* (1984) 168–73.

<sup>71</sup> See R Nimmer, ‘A Riff on Fair Use’ (2000) 148 *University of Pennsylvania Law Review* 738–40; H Travis, ‘Comment — Pirates of the Information Infrastructure: Blackstonian Copyright and the First Amendment’ (2000) 15 *Berkeley Technology Law Journal*, 777, 861; and Y Benkler, ‘Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain’ (1999) 74 *New York University Law Review* 354, 421.

<sup>72</sup> The term ‘other subject matter’ is put to one side for the purposes of this argument.

However, this argument distracts us from a much larger issue — the de facto copyright effect. That is, if a technological protection measure (such as, encryption) is applied to certain material, it is impossible to determine whether that material is a work for the purposes of copyright law *prior* to decrypting or circumventing the technological protection measure. Accordingly, if an alphabetical database which would otherwise fall outside the scope of copyright law is protected by encryption, it may in practice enjoy de facto copyright protection. This situation will arise as users may be reluctant to decrypt the file because one cannot be certain of infringement until circumvention has occurred. The defacto copyright protection issue is not one that appears to have received any legislative attention prior to the enactment of the recent amendments to the Australian *Copyright Act*, yet is an issue that strikes at the very heart of copyright law.

Consequently, the cause of action in s 116A is an extremely powerful tool that copyright owners of digital products can use against those that infringe their rights in those products. Also, on a practical note, if a technological protection mechanism is highly effective it will render consideration of commencing proceedings under s 116A irrelevant.<sup>73</sup> However, the technological protection measure provisions raise many issues that may require legislative or judicial attention before we can record with confidence how far the copyright pendulum has swung in favour of copyright owners.

### ***Electronic rights management information***

In contrast to the technological protection measures provisions, new provisions dealing with electronic rights management information appear to raise less contentious issues. Further, the application of these provisions to specific fact scenarios would appear to be a much easier exercise.

[28] The *Copyright Act* now provides remedies to copyright owners and their exclusive licensees against persons who intentionally remove or alter *electronic rights management information* (ERMI) and engage in certain dealings with works or other subject matter which has its ERMI removed or altered. ERMI is defined in s 10(1) as:

---

<sup>73</sup> Unfortunately, though the more effective a technological protection measure the more attractive a challenge it poses to the hacker community. The Secure Digital Music Initiative (SDMI) for digital music

- (a) information attached to, or embodied in, a copy of a work or other subject matter that:
- i. identifies the work or other subject matter, and its author or copyright owner; or
  - ii. identifies or indicates some or all of the terms and conditions on which the work or subject matter may be used, or indicates that the use of the work or other subject matter is subject to terms or conditions; or
- (b) any numbers or codes that represent such information in electronic form.

Arguably, merely attaching the text ‘©2000. All Rights Reserved’ on any electronic version of this article could fall within the scope of this definition. However, in many cases more sophisticated technological means will be employed. One sophisticated technique for attaching ERMI to copyright material will be the use of digital watermark technology.

Digital watermarks are an application of steganography.<sup>74</sup> The basic concept is to hide bits of data in a ‘carrier’ file (that is, the copyright work) so that those bits can be reassembled to reveal who owns a particular work and, depending on the technology used, who purchased the work.<sup>75</sup>

A civil action will lie under s 116B of the *Copyright Act* where:

- a person removes or alters ERMI;<sup>76</sup>
- without the permission of the owner or exclusive licensee;<sup>77</sup> and
- the person knew or ought reasonably to have known that the removal or alteration would induce, enable, facilitate or conceal an infringement of the copyright in the work or other subject matter.

It appears likely that proving whether ERMI has been altered or removed will be relatively straightforward. However, proving on the balance of probabilities that the defendant removed or altered ERMI may, as with all cases where computer evidence is involved, prove considerably more difficult.

---

products and the Content Scrambling System (CSS) for DVDs were both successfully hacked only a short time after being made available to the hacking community.

<sup>74</sup> Schneier, above n 39, 248. For an introduction to steganography see Denning, above n 8, 310–13.

<sup>75</sup> Schneier, above n 39, 249.

<sup>76</sup> See *Copyright Act* s 116B(1)(a).

<sup>77</sup> See *Copyright Act* s 116B(1)(b).

If a plaintiff can show on the balance of probabilities that a defendant did in fact remove or alter ERMI attached to or embodied in copyright material, it can then rely on the reversal of onus provision in s 116B(3) to satisfy the third element of the cause of action contained in s 116B.

Where a plaintiff cannot show that a defendant actually removed or altered ERMI, the plaintiff may consider bringing an action under s 116C. That section prohibits commercial and other dealings with copyright material which has had its ERMI removed or altered irrespective of whether the person dealing with the copyright material actually removed or altered the ERMI.

The cause of action under s 116C will be available if:

- (a) a person does any of the following acts in relation to a work or other subject matter in which copyright subsists without the permission of the owner or exclusive licensee of the copyright:
  - i. distributes for the purpose of trade a copy of the work or other subject matter;
  - ii. imports into Australia a copy of the work or other subject matter for the purpose of trade;
  - iii. communicates a copy of the work or other subject matter to the public; and
- (b) any electronic rights management information attached to the copy has been removed or altered; and
- (c) the person knew that the electronic rights management information has been so removed or altered without the permission of the owner or exclusive licensee of the copyright; and [29]
- (d) the person knew, or ought reasonably to have known, that the act referred to in paragraph (a) that was done by the person would induce, enable, facilitate or conceal and infringement of the copyright in the work or other subject matter.<sup>78</sup>

This prohibition is limited to the distribution, importation and communication of copyright material with ERMI removed. In addition, distribution and importation must be in the course of 'trade'. Accordingly, it will be possible for individuals to import

---

<sup>78</sup> See *Copyright Act* s 116C(1).

copies of copyright material with the ERMI removed or altered for *personal* use without falling foul of s 116C.<sup>79</sup>

While s 116C also contains reversal of onus provisions,<sup>80</sup> there is an important concession made by Parliament in relation to the level of knowledge required of defendants where they deal with copyright material which has ERMI removed or altered. The combined effect of ss 116C(1)(c) and 116(3)(a) is that a defendant will only be presumed to have *actual* knowledge of the removal or alteration of ERMI. Although no defendant enjoys having to rebut a presumption, it will be easier for a defendant to disprove knowledge on this issue than disproving constructive knowledge as well.

While many defendants may plead ignorance, what will probably occur in practice in some cases is that copyright owners will send letters of demand to alleged infringers. These will request alleged infringers to cease and desist trading in the copyright owner's material which has had the ERMI removed or altered. If the defendant fails to comply with such a letter of demand, it will be highly unlikely that she will be able to rebut the presumption in s 116C(3).

### ***Remedies for a breach of ss 116A, 116B or 116C***<sup>81</sup>

The remedies available for a breach of ss 116A, 116B or 116C are in line with those available in cases where other intellectual property rights have been infringed. They include:

- injunctions and either damages or an account of profits;<sup>82</sup> and
- additional damages.<sup>83</sup>

A court may award additional damages where it considers that the circumstances of the case (including the flagrancy of the breach and any benefit that the defendant may have acquired) make such an award appropriate.<sup>84</sup>

---

<sup>79</sup> Escaping liability under s 116C does not mean that such an act will not infringe other copyright or contractual rights of the copyright owner, though.

<sup>80</sup> See *Copyright Act* s 116C(3).

<sup>81</sup> Please note that criminal sanctions may also apply: see *Copyright Act* s 132(5A).

<sup>82</sup> See *Copyright Act* s 116D(1).

<sup>83</sup> See *Copyright Act* s 116D(2).

<sup>84</sup> *Ibid.*

## **Conclusion**

It is clear that the recent amendments to the *Copyright Act* will tip the balance of favour of copyright owners who supply their works or other subject matter in digital form to the market. Indeed, at least in relation to the provisions relating to technological protection measures, the potential exists for the amendments to the *Copyright Act* to alter the fundamental balance that copyright law has sought to strike between users and owners since the very notion of copyright was conceived.

What is unclear, however, is whether this variation in the balance is justifiable. The ability of copyright owners to apply technological protection measures to digital works and extinguish fair dealing rights and other user rights are perhaps examples of the Australian Parliament striking the wrong balance. Further, the new laws may unjustifiably hinder electronic security providers which in turn may lower the security of [30] the internet. A less secure internet is not in the interest of copyright owners because it will increase the potential for their works to be copied by pirates. These issues must be monitored closely to determine whether further amendments are required to enhance the functionality of Australian copyright law.