4

Enforcement measures

Introduction

4.1 The Bill introduces a number of measures designed to prevent the infringement of copyright in the digital domain. The measures arise from new technological safeguards that are currently used to identify and protect copyrighted material. Before being able to assess the measures and their implications, it is necessary to examine the technological safeguards to which they relate.

Technological safeguards

4.2 The two types of technological safeguards referred to in the Bill are electronic rights management information and effective technological protection measures.

Electronic rights management information

4.3 Item 9 of the Bill inserts a definition of electronic rights management information in the following terms:

> ***electronic rights management information*** means:
>
> (a) information attached to, or embodied in, a copy of a work or other subject-matter that:
>
> (i) identifies the work or subject-matter, and its author or copyright owner; and

(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 subject-matter is subject to terms or conditions; or

(b) any numbers or codes that represent such information in electronic form.

4.4 The Explanatory Memorandum states that electronic rights management information typically includes details about the copyright owner and the terms and conditions of the use of the material. The Government intends that electronic rights management information will include 'digital watermarks'.[1]

4.5 The Australian Record Industry Association (ARIA) and the Phonographic Performance Company of Australia Ltd (PPCA) in their joint submission stated that the definition in the Bill may be too limited.[2] They argued that the requirement that information satisfy both subparagraphs (i) and (ii) of paragraph (a) in order to qualify as electronic rights management information is overly prescriptive, and inconsistent with the terms of the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT).

4.6 In the context of sound recordings and performances, article 19(2) of the WPPT defines electronic rights management information to include information which identifies the phonogram or the producer of the phonogram and the performer or the performance of the performer. ARIA and PPCA argued that in order to achieve conformity with the international standard, these elements should be added to the proposed definition of electronic rights management information.[3] In this regard the Committee notes that sound recordings are dealt with in Part IV of the Copyright Act, and so come within the category 'subject matter' already provided for in the proposed definition of electronic rights management information.

4.7 The International Intellectual Property Alliance (IIPA) supports the recommendations of ARIA and PPCA, acknowledging that the Bill generally 'does a good job' of meeting the obligation to protect the integrity of electronic rights management information as required by the WCT and WPPT.[4]

---

1 Explanatory Memorandum, p. 22.

2 Australian Record Industry Association (ARIA) and Phonographic Performance Company of Australia (PPCA), *Submissions*, p. S485.

3 ARIA & PPCA, *Submissions*, p. S485.

4 International Intellectual Property Alliance (IIPA), *Submissions*, p. S444.

Conclusion

4.8 The Committee considers the amendments proposed by ARIA and PPCA to be sound. As there were no objections to the proposed amendments to the definition of electronic rights management information, the Committee is persuaded that they should be accepted.

Recommendation 10

4.9 **The Committee recommends that item 9 of the Copyright Amendment (Digital Agenda) Bill 1999 be amended by replacing the word 'and' appearing at the end of proposed subparagraph (a)(i) of the definition of 'electronic rights management information' with the word 'or'.**

Recommendation 11

4.10 **The Committee further recommends that item 9 of the Copyright Amendment (Digital Agenda) Bill 1999 be amended so that subparagraph (a)(i) of the definition of 'electronic rights management information' reads 'identifies the work or subject matter, and its author, producer, or copyright owner; or in the case of a performance, the performance and the performer'.**

Effective technological protection measures

4.11 Evidence to the Committee indicated that technological measures to protect copyrighted materials are essentially of two types: access control measures and copy control measures.[5] Access control measures allow the copyright owner to control who has access to the copyrighted material. Examples of access control measures include password protections, file permissions and encryption. Copy control measures allow the copyright owner to control the extent of a person's access to copyrighted material. Copy control measures are based on the premise that a user already has some lawful access to the work, and the measures seek to control what the user can then do with the lawfully obtained copyrighted material.[6] An

5 Steven Metalitz, IIPA, *Transcript*, p. 176.

6 The term 'copy control measure' is somewhat misleading, as was pointed out to the Committee in evidence. 'Copy control measure' refers to a mechanism which controls any act comprised

example of a copy control mechanism is a mechanism that allows first generation copies but prevents second and subsequent generation copies.[7]

4.12 As was pointed out to the Committee, there is a difference in scope between the two types of measures. Copy control measures are more closely allied with copyright, and with the infringement of copyright, than access control measures.[8] Access control measures seek to prevent all access to copyright material, not only that access which is unlawful.

Purpose of effective technological protection measures

4.13 This difference in scope between access and copy control measures gave rise to argument before the Committee between copyright owners and copyright users as to how far the definition of effective technological protection measure should extend. The copyright users maintained that linking protection measures to copyright infringement was critical. They argued that to include access control measures in the definition of effective technological protection measure would be to extend the reach of copyright law, rather than to merely enforce it.[9]

4.14 Copyright users expressed the further concern, with which the Committee sympathises, that the wider definition (including access control measures) has the potential to seriously threaten the continued existence of the public domain.[10] The copyright owners replied that as a practical matter, the threat posed by access control measures to the public domain is minimal.[11] The issue of the impact of protection measures on the public domain arises more generally in the context of the exceptions to the enforcement provisions, and further discussion of this issue will be deferred until the exceptions are canvassed (see below).

4.15 There was also some argument before the Committee as to whether or not the applicable international treaties (the WCT and the WPPT) require domestic legislation to prescribe interference with access control measures, in addition to copy control measures. The copyright users asserted that the treaties did not require the inclusion of access control measures in the definition of effective technological protection measure,[12]

---

in the copyright, not only the reproduction right. See the comments of Steven Metalitz, IIPA, *Transcript*, p. 195.

7 Steven Metalitz, IIPA, *Transcript*, p. 176.

8 Steven Metalitz, IIPA, *Transcript*, p. 176.

9 Jamie Wodetzki, Australian Digital Alliance (ADA), *Transcript*, p. 178.

10 Jamie Wodetzki, ADA, *Transcript*, pp. 191–92.

11 Steven Metalitz, ADA, *Transcript*, p. 194.

12 Jamie Wodetzki, ADA, *Transcript*, p. 178.

while the copyright owners maintained the opposite view. The copyright owners further noted that the wider definition is consistent with the positions taken by the US and the European Community (EC).[13]

Definition of effective technological protection measure

4.16 Against this background the Committee considered the definition of effective technological protection measure contained in the Bill. Item 4 inserts the following definition:

> ***effective technological protection measure*** means a device or product, or a component incorporated into a process, that is designed to prevent or inhibit the infringement of copyright subsisting in a work or other subject-matter if, in the ordinary course of its operation, access to the work or other subject-matter protected by the measure 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 in a work or other subject-matter.

4.17 This definition condenses items 14 and 18 of the Exposure Draft of the Bill. The Explanatory Memorandum indicates that the proviso 'if, in the ordinary course of its operation' was inserted to ensure that the argument cannot be advanced that a measure is not an effective technological protection measure because access has in fact been gained through unlawful means.[14] The Committee notes ARIA's and PPCA's concern that the proviso may undermine the whole definition,[15] but does not share that concern. Similarly, the Committee is aware of, but does not share, the Law Council of Australia's concern that the proviso introduces a logical flaw into the definition.[16]

4.18 The Committee received submissions to the effect that the new definition of effective technological protection measure lacks clarity[17] and that it is probably ineffective.[18] The IIPA argues that the definition betrays a lack of understanding as to how many copy control protection measures work.

---

13 Steven Metalitz, IIPA, *Transcript*, p. 176; see s. 1201(a) of the *Digital Millennium Copyright Act* (US) and art 6 of the Amended Proposal for EU Directive on the Harmonisation of certain aspects of copyright and related rights in the information society.

14 Explanatory Memorandum, p. 21.

15 ARIA and PPCA, *Submissions*, p. S485.

16 Law Council of Australia, *Submissions*, p. S473.

17 System Administrators Guild of Australia (SAGE-AU), *Submissions*, p. S4.

18 IIPA, *Submissions*, p. S440.

The definition encompasses only those protection measures that operate by controlling access by an access code or process, and for the purposes of preventing infringement.

4.19 In the view of the Committee, the definition of effective technological protection measure in the Bill is a hybrid of access control and copy control measures, as those terms have been described above. For this reason the Committee does not consider the proposed definition of effective technological protection measure ineffective. However, in the Committee's view, it may be preferable to define effective technological protection measure simply in terms of copy control measures. In other words, an effective technological protection measure is a device or product, or component incorporated into a process, that, in the ordinary course of its operation, is designed to prevent or inhibit the infringement of copyright subsisting in a work or other subject-matter.

4.20 ARIA and PPCA submitted that the definition of effective technological protection measure should refer to components of a device, in addition to the existing 'components of a treatment'.[19] The Committee understands these arguments but does not consider that there is a real danger of injustice resulting from the existing definitions.

Circumvention device and service

4.21 There is one other pair of definitions that is relevant to the enforcement measures introduced by the Bill. They are 'circumvention device' and 'circumvention service', which make use of the term 'effective technological prevention measure'. Proposed Division 2A of Part V goes on to make certain activities, in relation to circumvention devices and services, civil and criminal offences.

4.22 Item 4 inserts the following definition of circumvention device (item 5 inserts a similar definition in respect of circumvention services):

> ***circumvention device*** means 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.

4.23 Copyright owners submitted that under the proposed definition, a device which has many purposes (a multi-purpose device), one of which is circumvention of an effective technological protection measure, may not

19 ARIA & PPCA, *Submissions*, p. S484.

be categorised as a circumvention device.[20] The copyright owners argued that this leaves the way open for pirates to produce and trade in devices, which they may even openly market as circumvention devices, but which will not be caught by the enforcement measures.[21] They therefore submitted that the definition should include devices whose primary purpose or use is the circumvention, or facilitation of the circumvention, of effective technological protection measures, as well as devices which are marketed as circumvention devices.

4.24 The Committee recognises that the force of this argument depends on both the construction that is given to the phrase 'limited commercially significant purpose or use', and on the exceptions that are provided to the enforcement provisions. However, the Committee agrees that it is desirable to include in the definition of circumvention device a reference to devices whose primary purpose is, or devices which are marketed as, circumvention devices.

Recommendation 12

4.25 **The Committee recommends that the meaning of circumvention device in item 4 of the Copyright Amendment (Digital Agenda) Bill 1999 be amended to specifically include devices whose primary purpose or use is the circumvention, or facilitating the circumvention, of an effective technological protection measure, and devices which are promoted, advertised, or marketed as having the purpose of circumventing an effective technological protection measure.**

How should technological safeguards be protected?

4.26 In the course of hearing evidence, the Committee soon appreciated the wide divergence that exists between the views of the copyright owners on the one hand, and the copyright users on the other. At their most extreme positions, the copyright owners wish to manage all access to copyrighted material, both lawful and unlawful, apart from access for a few enumerated, legitimate purposes. Conversely, the copyright users wish to have uncontrolled access to all copyrighted material, and leave the

20 ARIA & PPCA, *Submissions*, p. S484; IIPA, *Submissions*, p. S441.

21 IIPA, *Submissions*, p. S441.

copyright owners to obtain redress for any consequent infringement of their copyright through infringement actions.

4.27 The Committee considers this a useful framework for considering the issues that arise in connection with the enforcement measures contained in the Bill. The extent of the proposed enforcement measures, and the scope of their exceptions, directly affect the balance that the Copyright Act strikes between the interests of copyright owners and users.

4.28 The enforcement measures relate to the two types of technological safeguards, electronic rights management information and effective technological protection measure, discussed above. The provisions in relation to each technological safeguard will be discussed firstly, and then some general concerns about the enforcement provisions will be canvassed.

Enforcement provisions in relation to electronic rights management information

4.29 The Bill creates, in proposed section 116B, civil liability for removing or altering electronic rights management information attached to copyrighted material, without the permission of the owner or licensee of the copyright, when the person removing or altering the electronic rights management information knew, or ought reasonably to have known, that it would induce, enable, facilitate or conceal the infringement of the copyright.

4.30 Proposed section 116B has been added since the Exposure Draft of the Bill. The joint submission from the Attorney-General's Department and the Department of Communications, Information Technology and the Arts (AGD and DCITA) indicated that the addition was made on the suggestion of copyright owners.[22] Copyright owners support the creation of civil liability.[23]

4.31 Copyright owners submitted to the Committee that intent to remove or alter electronic rights management information should be an alternative element of the civil offence created by proposed s. 116B. The Committee agrees with this submission.

4.32 Proposed section 116C creates civil liability for distributing, importing or communicating any copyrighted material from which electronic rights

22 Attorney-General's Department and Department of Communications, Information Technology and the Arts (AGD & DCITA), *Submissions*, p. S602.

23 IIPA, *Submissions*, p. S444; ARIA & PPCA, *Submissions*, p. S492.

management information has been removed, when the person distributing, importing or communicating it

- knew that the electronic rights management information had been so removed, and
- knew or ought reasonably to have known that the removal of the electronic rights management information would induce, enable, facilitate or conceal the infringement of the copyright.

4.33 Copyright owners submitted that liability should attach if the person distributing, importing or communicating knew or ought reasonably to have known that electronic rights management information had been removed.[24] In the opinion of the Committee, this represents an appropriate extension of civil liability.

Recommendation 13

4.34 **The Committee recommends that proposed section 116C(1)(c) of the Copyright Amendment (Digital Agenda) Bill 1999 be amended to provide that 'the person knew or ought reasonably to have known that the electronic rights management information had been so removed or altered without the permission of the owner or licensee of the copyright'.**

Enforcement provisions in relation to effective technological protection measures

4.35 In the Bill, effective technological protection measures are protected by prohibitions on various activities in relation to circumvention devices. The prohibitions, contained in proposed s. 116A(1)(b), relate to the manufacture of, and commercial dealing in, circumvention devices, including their distribution and importation for trade and other purposes prejudicial to the copyright owner. Proposed section 116A(1)(b) also prohibits providing a circumvention service and making circumvention

24 ARIA & PPCA, *Submissions*, p. S492; ARIA & PPCA, Business Software Association of Australia (BSAA), Australian Performing Right Association (APRA), Motion Picture Association (MPA), IIPA, Australian Publishing Association (APA), correspondence to the Committee, 21 October 1999, 'Copyright Amendment (Digital Agenda) Bill Suggested Amendments'.

devices available online to the extent that it will prejudicially affect the copyright owner.

Use of circumvention devices

4.36 The Bill does not prohibit the use of circumvention devices per se. Storage Technologies Australia (Store Tek) regarded a prohibition on use, rather than availability, as necessary to maintain the existing balance in the Copyright Act between the interests of copyright owners and users.[25]

4.37 Copyright owners urged the Committee that the Bill should contain a blanket prohibition on the use of circumvention devices.[26] Such a prohibition, they argued, would be consistent with approaches taken in the United States and the European Community,[27] and would meet the requirements of the WCT and the WPPT. The copyright owners further submitted that the prohibition is necessary in order to adequately protect copyrighted materials.

4.38 Contrary to the views of the copyright owners, AGD and DCITA, suggested that the enforcement measures of the Bill 'will provide copyright owners with a powerful tool to combat online piracy'.[28] They explained the Government's rationale for banning manufacture and dealing in circumvention devices, but not their use as follows:[29]

> The government believes that the most significant threat to copyright owners' rights lies in preparatory acts for circumvention, such as manufacture, importation, making available online and sale of devices, rather than individual acts of circumvention.

4.39 There was some discussion before the Committee about the practical efficacy of the enforcement measures in respect of circumvention devices. The Business Software Association of Australia submitted that they are 'virtually impossible to enforce in practice because you have to prove essentially that the person is supplying the device for a prohibited purpose'.[30] AGD and DCITA pointed out that the enforcement of the measures will mainly occur in relation to public and commercial activities,

25 Storage Technology of Australia, *Submissions,* p. S232.

26 ARIA & PPCA, *Submissions,* p. S491; APA, Submissions, p. S402.

27 See article 6 of the Amended Proposal for a European Parliament and Council Directive on the harmonisation of certain aspects of copyright and related rights in the information society and the *Digital Millennium Copyright Act* (US).

28 AGD & DCITA, *Submissions,* p. S612.

29 AGD & DCITA, *Submissions,* p. S612.

30 Maurice Gonsalves, BSAA, *Transcript,* p. 183.

in contrast to sanctions against use which would necessitate intervention in the private sphere.[31] On this point the Committee is persuaded that enforcement measures should target manufacture and supply in the commercial world, rather than private use.

4.40 AGD and DCITA also acknowledged that a ban on the use of circumvention devices 'could prevent users carrying out otherwise lawful activities, particularly with respect to IT security testing'.[32] The Committee notes that in its submissions, the Systems Administrators Guild of Australia (SAGE-AU) argued that the existing provisions (banning the manufacture and dealing in circumvention devices) in fact prevents IT security testing in any event. The issue of the need for an exception for systems administration and security testing will be explored below.

4.41 The Committee received evidence from copyright users who were opposed to any ban on circumvention devices.[33] They maintained that circumvention devices and services should be available to any person who requires the device or service for a non-infringing purpose.[34] They argued that even if a person is able to obtain a device and use it without breaching the existing prohibition on dealing in devices, a copyright owner will still be able to bring an action against any person who goes on to infringe the copyright.[35]

4.42 Copyright users were concerned that a prohibition on the use of circumvention devices would not only be an effective enforcement measure, but would be a vehicle for expanding the rights comprised in copyright beyond those contained in the Copyright Act.

Conclusion

4.43 The Committee notes the comments made by AGD and DCITA, that this is a new area of law, to regulate an aspect of rapidly developing technology.[36] The Committee considers it premature to alter the existing balance between the interests of copyright owners and users when extending into the digital domain. This does not mean that adjustments will never be required, but the Committee thinks it prudent to delay possibly altering the balance until the ramifications of copyright in the

31 AGD & DCITA, *Submissions*, p. S612.

32 AGD & DCITA, *Submissions*, pp. S612–13.

33 Supporters of Interoperable Systems in Australia (SISA), *Submissions*, p. S286; ADA, *Submissions*, p. S278; Australian Consumers' Association (ACA), *Submissions*, p. S391.

34 ADA, *Submissions*, p. S278.

35 SISA, *Submissions*, p. S286.

36 AGD & DCITA, *Submissions*, p. S612.

emerging digital age are better and more widely understood. For this reason the Committee considers a ban on the use of circumvention devices for all purposes inappropriate.

4.44 The Committee supports the existence of a civil remedy for the use of a circumvention device for the purposes of infringing copyright. The Committee notes that the Copyright Act already contains a civil remedy for the infringement of copyright. That remedy is available when infringement occurs in any way at all, including through the use of a circumvention device. In the Committee's opinion, there should be in addition a civil remedy where a person uses a circumvention device in an attempt to infringe copyright.

Recommendation 14

4.45 **The Committee recommends that item 98 of the Copyright Amendment (Digital Agenda) Bill 1999 be amended to include a provision making it a civil offence to intentionally use a circumvention device for the purpose of infringing copyright in a work or other subject matter, regardless of whether the copyright in the work or other subject matter is infringed.**

In addition to any relief it grants, a court should have a discretion to order that the defendant pay to the Commonwealth an appropriate pecuniary penalty.

When may effective technological protection measures be circumvented?

4.46 The Committee recognises that the exceptions to a rule are as equally important as the rule itself, and thus the Committee is concerned to ensure that the exceptions provided to the prohibition on the manufacture and dealing in circumvention devices are also necessary and sufficient.

4.47 There are two types of exceptions in the Bill. The first is the so-called 'permitted purposes' exception, which requires the person claiming the exception to make a declaration. In addition to the exception for permitted purposes, the Bill contains unqualified exceptions for the purposes of law enforcement and national security.

4.48 Evidence to the Committee showed that there were two main areas of concern with respect to the exceptions. Firstly, the scope of the exceptions themselves — including using a circumvention device for a permitted purpose — and secondly, the way in which the exceptions are implemented. Each of these will be examined in turn.

Permitted purposes

4.49 The effect of proposed section 116A(3) and (4) is that civil liability does not arise when a circumvention device or service is used for certain 'permitted purposes'. Proposed section 116A(7) specifies those permitted purposes to be when:

> (a) the device or service is used for the purpose of doing an act comprised in the copyright in a work or other subject-matter; and
>
> (b) the doing of the act is not an infringement of the copyright in the work or other subject-matter under section 47D, 47E, 47F, 49, 50, 183 or Part VB.

4.50 The permitted purposes exception also applies in relation to criminal offences: see ss 132(5G)–(5J).

4.51 The Exposure Draft of the Bill did not contain any mention of 'permitted purposes'. AGD and DCITA explained that the permitted purposes exception has been introduced to counterbalance another change made to the Exposure Draft, namely the enlarging of the mental requirement in respect of the civil liability from recklessness to constructive knowledge.[37] The permitted purposes exception is designed to ensure that effective technological protection measures are not used to restrict the scope of the recognised exceptions to copyright infringement contained in the Copyright Act, and to ensure reasonable access to copyright material in electronic form.[38]

4.52 The permitted purposes exceptions cover educational institutions (Part VB), the Crown (s. 183), and library (ss 49 and 50) exceptions. The reproduction of computer programs to achieve interoperability and for security testing and error correcting (ss 47D–E) are also permitted purposes. This set does not represent all the exceptions to infringement under the Copyright Act.

37 AGD & DCITA, *Submissions*, p. S601.

38 AGD & DCITA, *Submissions*, p. S614.

4.53 As may be expected, copyright users advocated the expansion of permitted purposes to include all non-infringing purposes,[39] while copyright owners opposed exceptions for permitted purposes altogether.[40]

4.54 The copyright owners argued that the permitted purposes exception 'guts' enforcement measures in relation to effective technological protection measures.[41] They argued that it would generate a market in circumvention devices and services, which would quickly develop into a black market for pirates.[42] They further submitted that a prohibition on the manufacture and dealing in circumvention devices and services would not restrict the operation of the exceptions to infringement contained in the Copyright Act. This is because the Bill does not prohibit the use of such devices and services.

4.55 This argument does not find favour with the Committee. There is a need to allow copyright users to use circumvention devices in pursuit of legitimate purposes, such as system administration and library collection preservation. Leaving to one side the issue of whether such devices can be used without some form of adaptation — such adaptation being the making of a new circumvention device, there is the objection that in principle, users should not be deprived of innovative Australian circumvention devices for uses other than the infringement of copyright.[43] In view of the need to ensure the continued operation of the exceptions to infringement, the Committee concludes that the permitted purposes exception should remain. The issue that remains to be considered is how far the permitted purposes exception should extend.

4.56 SISA pointed out that under the Exposure Draft of the Bill, civil and criminal liability only arises if the purpose for making or dealing in a circumvention device is to infringe copyright. Therefore in the Exposure Draft, all non-infringing purposes are permitted purposes. SISA noted that no explanation has been given as to why only a subset of these are specified as permitted purposes in the Bill.[44] The Committee concludes that subject to the other exceptions considered below, that an appropriate balance between copyright owners and users has been struck in specifying key non-infringing uses as permitted purposes.

---

39 ADA, *Submissions*, p. S278.

40 IIPA *Submissions*, pp. S442–43; ARIA, BSAA, APRA, MPA, IIPA, PPCA & APA - correspondence to the Committee, 21 October 1999, 'Copyright Amendment (Digital Agenda) Bill Suggested Amendments' pp. 4, 5, 10.

41 IIPA, *Submissions*, p. S442.

42 IIPA, *Submissions*, p. S443.

43 SAGE-AU, *Submissions*, p. S5.

44 SISA, *Submissions*, p. S284; see also Storage Technology of Australia, *Submissions*, p. S233.

Other possible permitted purposes

4.57 Various industry groups have suggested to the Committee that additional exceptions are required to allow for the manufacture and supply of circumvention devices in specific circumstances.

4.58 An initial issue that arises is whether the suggested additional exceptions should be included as permitted purposes, in which case signed declarations would be required before circumvention devices and services could be supplied, or whether they should be exceptions in their own right.

4.59 In the Committee's view it is appropriate that the proposed exceptions, for system administration and library collection preservation, be included in the Bill as permitted purposes. This will reduce the possibility of the exceptions being abused and will help to maintain the balance between the interests of copyright owners and users that has been struck in the Copyright Act.

System administrators

4.60 System administrators are people who are responsible for investigating and resolving technical problems in computer systems, and for maintaining the operational integrity and security of such systems.[45] Examples of system administrators include IT departments and Internet Service Providers (ISPs). SAGE-AU submitted that the Bill's enforcement measures prevent system administrators from carrying out their professional functions.

4.61 There was some discussion before the Committee about the precise nature of a system administrator's functions, and whether those functions could be carried out under the Copyright Act amended as proposed. In other words, could system administrators operate effectively without manufacturing or dealing in circumvention devices, or providing circumvention services, and if not, then can they bring their operations within one of the permitted purposes exceptions?

4.62 The Committee notes that 'manufacture' is not defined in the Act or the Bill. SAGE-AU was of the view, with which the Committee agrees, that system administrators are involved in the manufacture of circumvention devices to the extent that they need to create them. They may also deal with circumvention devices in contravention of the proposed amendments in the Bill.

45 SAGE-AU, *Submissions*, pp. S579, S583.

4.63 It will therefore be necessary for system administrators to establish that they manufacture circumvention devices for a permitted purpose. Discussion before the Committee focussed on one of the existing permitted purposes in particular that may cover the operations of systems administrators, namely, s. 47F, security testing. Section 47F permits the reproduction of a legitimate copy of a computer program with the permission of the owner or licensee of the program, for the purposes of testing in good faith the security of a computer system, or for investigating and correcting a security flaw.

4.64 The IIPA argued that those functions which did not fall within the category of security testing in s. 47F, could be covered by the terms of the licence agreement.[46]

4.65 One technology lawyer argued that s. 47F itself is too narrowly drafted to include many types of security testing, let alone other systems administration activities.[47] Ms Anne Fitzgerald pointed out that on a daily basis, security testing organisations are required to examine pirated software, software developed by a recognised software vendor which has been modified by an intruder to fulfil some other purpose, and software that has been developed by an intruder or hacker to exploit a vulnerability in a computer system. Under existing s. 47F these activities are prohibited.

4.66 The Committee agrees that s. 47F should be amended to permit security testing to be done without the permission of the owner or licensee, and on infringing copies of computer programs. In addition, the Committee understands that computer files, as well as computer programs, can be used as tools to attack the security of a computer system. The Committee therefore concludes that s. 47F should be amended to cover computer files as well. Furthermore, the Committee is aware that tools for attacking computer systems are constantly being developed. For this reason the Committee believes that the adequacy of the exception for security testing should be reviewed in the proposed three year review.

46 Steven Metalitz, IIPA, *Transcript*, p. 186.

47 Anne Fitzgerald, *Submissions*, pp. S167–69.

Recommendation 15

4.67 **The Committee recommends that section 47F of the *Copyright Act 1968* be amended as follows:**

Delete paragraph (1)(a).

Replace paragraph (1)(d) with

(1)(d) the information resulting from the making of the reproduction or adaptation is not readily available from another source when the reproduction or adaptation is made.

Replace subsection (2) with:

(2) Subject to this Division, the copyright in a work that is in electronic form (the original copy) is not infringed by the making of a reproduction or adaptation of the work if:

(a) the reproduction is made for the purpose of investigating in good faith the security threat posed to a computer system or network by the introduction of the original copy into the system or network; and

(b) the reproduction or adaptation is made only to the extent reasonably necessary to achieve a purpose referred to in paragraph (a); and

(c) the information resulting from the making of the reproduction or adaptation is not readily available from another source when the reproduction or adaptation is made.

A specific exception?

4.68 SAGE-AU submitted that security testing formed only a small part of the functions of system administrators.[48] For this reason they argued that a separate exception was required. SAGE-AU's submission to the Committee contained two suggestions for a proposed system administration exception.[49] The first proposal exempts the activity of

48 Geoff Halprin, SAGE-AU, *Transcript*, p. 185.

49 SAGE-AU, *Submissions*, pp. S580, S581.

systems administration. 'Systems administration' is broadly defined to include the management of computer systems. The second proposal exempts the class of system administrators.

Conclusion

4.69 The Committee has carefully considered the need for a specific exemption to allow system administrators to create circumvention devices in pursuit of their functions that extend beyond security testing. The Committee notes that the use of circumvention devices is itself not prohibited. The Committee further believes that any civil action brought against a system administrator for manufacturing a circumvention device or providing a circumvention service in the proper pursuit of his or her functions would be dismissed by the courts with nominal damages. Similarly, any criminal trial for such an offence would be quickly dismissed.

4.70 Strong principles of public policy dictate that actions brought against system administrators should not succeed, and the Committee is confident that the courts will take those principles into account in disposing of any actions. In the Committee's view, there is no incentive for copyright owners to sue system administrators, nor any incentive for them to be prosecuted. The Committee therefore concludes that a specific exemption, from the potential liability imposed by proposed ss 116A, 132 (5B) and (5C), is probably unnecessary.

4.71 However, the Committee thinks it desirable that the Attorney-General refers to those principles of public policy and clearly states that proposed ss 116A, 132(5B) and (5C) are not intended to apply to system administrators in the proper pursuit of their functions. Furthermore, the Committee wishes to encourage the system administration industry to develop an industry code of practice that may in the future be given legislative backing.

Recommendation 16

4.72 **The Committee recommends that the Explanatory Memorandum to the Copyright Amendment (Digital Agenda) Bill 1999 be amended to clearly state that the legislature does not intend for system administrators acting in proper pursuit of their functions to be held liable under proposed ss 116A, 132(5B) or (5C).**

Recommendation 17

4.73 **The Committee recommends that should the systems administration industry have developed a well accepted industry code of practice by the time the Government conducts its proposed three year review of this legislation, the Government consider creating a permitted purpose exception to the manufacture and dealing in circumvention devices, based on that industry code of practice.**

Study of computer programs

4.74 SISA particularly supported the inclusion of s. 47B(3) of the Copyright Act as a permitted purpose. Section 47B(3) allows a person to copy or adapt a legitimate copy of a computer program in order to study the ideas behind the program and the way in which it functions. The Committee agrees that this activity could easily require the use of a circumvention device and hence s. 47B(3) should be included as a permitted purpose.

Preservation of library collections

4.75 The National Library of Australia drew the Committee's attention to the need for library officers to be supplied with, and to make, circumvention devices in order to carry out the task of preserving the library's collection in pursuit of its functions.[50] The Committee agrees that there is a need for such an exception, and that it can be created by including s. 51A as a permitted purpose.

Conclusion

4.76 The Committee concludes that additional permitted purposes need to be identified in the Bill in order to allow for the proper operation of existing exceptions to infringement. In particular, the Committee concludes that the manufacture and dealing in circumvention devices should be allowed for the purposes of studying the ideas behind a computer program, and for the purpose of creating a preservation copy of a manuscript or original artistic work.

50 Jasmine Cameron, National Library of Australia, *Transcript*, p. 199.

Recommendation 18

4.77 **The Committee recommends that items 98 and 100 of the Copyright Amendment (Digital Agenda) Bill 1999 be amended as follows: in proposed section 116A(7)(b) and in proposed subsection 132(5J)(b), omit 'under section 47D, 47E, 47F, 49, 50, 183 and Part VB' and insert 'under section 47B(3), 47D, 47E, 47F, 49, 50, 51A, 183 and Part VB'.**

Implementation of permitted purposes exception

4.78 The other aspect of the permitted purposes exception that attracted comment in evidence to the Committee was its practical operation. The comment focussed on proposed ss 116(3) and 132(5G), which require signed declarations to trigger the application of the exception. Specifically, with regard to supplying (selling, letting for hire or making available online) a circumvention device or service, the person being supplied must give the supplier a signed declaration stating that the device or service will only be used for a named permitted purpose, in order for the exception to apply.

4.79 In their joint submission, AGD and DCITA stated that

> The system of requiring declarations is not overly onerous and is necessary to ensure as far as possible that circumvention devices are only made for permitted purposes.[51]

4.80 Copyright owners argued that the system of signed declarations used in the Bill could be easily rorted by pirates.[52] This is especially so since the Bill does not provide any penalty for making a false declaration.[53]

4.81 The Committee agrees that in order to properly protect the rights of copyright owners, the permitted purposes exception needs to be underpinned by an effective sanction for the making of false declarations.

51 AGD & DCITA, *Submissions*, p. S614.

52 BSAA, *Submissions*, p. S59.

53 IIPA, *Submissions*, p. S443.

Recommendation 19

4.82 **The Committee recommends that new proposed section 116E be inserted into the Copyright Amendment (Digital Agenda) Bill 1999 as follows:**

116E False declarations

- **A person who makes a false declaration under sections 116A(3) or 132(5G) is guilty of an offence.**
- **The maximum penalty that can be imposed on a person convicted of an offence under subsection (1) is the penalty specified in the *Statutory Declarations Act 1959* for the making of a false statement in a statutory declaration.**

4.83 Mr Leif Gamertsfelder raised another concern with the system of signed declarations contemplated in proposed ss 116A(3) and 132(5G). He submitted that the system does not facilitate a proactive approach to system and network security.[54] Circumvention devices can only be supplied once a declaration is received, and the declaration will only be made once a problem is discovered. The Committee understands this concern, but in view of the absence of a ban on the use of circumvention devices, does not consider it to be problematic.

General concerns about enforcement provisions

Civil remedies

4.84 A number of submissions received by the Committee have contained comments regarding the provisions that create civil liability. These concerns relate to proposed ss 116A, B and C (item 98 of the Bill).

4.85 The first issue concerns the reversal of the onus of proof in proposed ss 116A(6), 116B(3) and 116C(3). As a result, in an action under these proposed sections, the defendant is required to prove that he or she did not know, and reasonably could not have known, that his or her actions would induce, enable, facilitate or conceal the infringement of copyright.

54 Mr Leif Gamertsfelder, *Submissions*, p. S378.

SISA and Storage Technology of Australia acknowledged that the reversal of the onus, coupled with the strengthened mental element, places the defendant in a weaker position than under the Exposure Draft.[55] The Law Council of Australia noted that although the reversal is arguably inconsistent with common law principles, it does not unduly prejudice the defendant.[56]

4.86 The Committee notes that the reversal of the onus of proof has been considered by the Senate Standing Committee for the Scrutiny of Bills.[57] The Scrutiny of Bills Committee did not comment adversely about the reversal. The Committee does not have any concerns of its own on the reversal and concludes that the reversal of the onus of proof in proposed ss 116A(6), 116B(3) and 116C(3) is acceptable.

4.87 The second issue is about the standing of persons to bring actions under proposed ss 116A(5), 116B(2) and 116C(2), presently the owner and licensee of the copyright. The IIPA submitted that the current standing requirement is too narrow, and that standing should be conferred on any injured party. The BSAA submitted the contrary, that the standing requirement is too broad, and that licensees should not be given standing. The Committee concludes that standing should be conferred on the copyright owner or any person authorised by the owner.

Recommendation 20

4.88 **The Committee recommends that item 98 of the Copyright Amendment (Digital Agenda) Bill 1999 be amended so that ss 116A(5), 116B(2) and 116C(2) provide that any person authorised by the owner of the copyright, may also bring an action against the person.**

4.89 The third issue, raised by copyright owners, was that proposed ss 116A(1)(b) and 116B(1)(b) effectively allow licensees to authorise the manufacture and distribution of devices to circumvent effective technological protection measures attached to an owner's material, and the removal or alternation of electronic rights management information attached to an owner's material, respectively.[58] They therefore

55 SISA, *Submissions*, p. S279.

56 Law Council of Australia, *Submissions*, p. S472; SISA, Submissions, p. S285; Storage Technology of Australia, *Submissions*, p. S232.

57 *Scrutiny of Bills Alert Digest No 14 of 1999, 22 September 1999.*

58 BSAA, *Submissions*, p. S60; Maurice Gonsalves, BSAA, *Transcript*, p. 205.

recommended the removal of the word 'licensee' from each subparagraph. In the Committee's view, adequate protection for copyright owners from this potential problem can be achieved through the terms of the licence agreement.

Criminal sanctions

4.90 There was also some discussion before the Committee in relation to the provisions establishing criminal sanctions. The requisite mental element required for the criminal offences established by proposed ss 132(5B)–(5E) is knowledge or recklessness.

4.91 The copyright owners submitted that constructive knowledge should be a sufficient mental element. In other words, criminal liability should attach if a person ought reasonably to have known that the manufacture, sale, distribution or importation of a circumvention device, or the removal or alteration of electronic rights management information, or the distribution, importation or communication of material whose electronic rights management information has been removed, would induce, enable, facilitate or conceal an infringement of its copyright.

4.92 The Committee notes that constructive knowledge is an element of the civil offences created in proposed ss 116A–C. In the Committee's view, it is appropriate that civil offences require a lesser degree of knowledge than criminal offences. For this reason the Committee concludes that constructive knowledge should not be an alternative mental element for the criminal offences in proposed ss 132(5B)–(5E).

4.93 The BSAA recommended the omission of proposed s. 132(5K), which deals with the evidential burden of proof for certain criminal offences.[59] The Committee also notes the dissatisfaction of the IIPA with respect to proposed s. 132(5K).[60] The Committee is unclear as to why copyright owners object to the proposed section which is designed to facilitate proof of the offence. In relation to this the Explanatory Memorandum states[61]

> It is believed that the matters referred to [in proposed s. 132(5K)] will be peculiarly within the knowledge of the defendant, and will be more costly for the prosecution to disprove than for the defence to establish.

59 BSAA, *Submissions*, p. S60.

60 IIPA, *Submissions*, p. S442.

61 Explanatory Memorandum, p. 58.

4.94 The Committee notes that the Senate Standing Committee for the Scrutiny of Bills has requested the Attorney-General to provide a further justification for placing an evidential burden on the defendant.[62] The Committee considers that the placing of a burden of proof on the defendant is reasonable in the circumstances and that proposed s. 132(5K) should be retained.

62 *Scrutiny of Bills Alert Digest No 14 of 1999, 22 September 1999.*