Cyberspace Law and Policy Centre
A Centre for the Public Interest in Networked Transactions

Submission on the exposure draft Bill on technological protection measures (TPMs)

Graham Greenleaf, Alana Maurushat, David Vaile, Catherine Bond and Abi Paramaguru
Cyberspace Law & Policy Centre
University of New South Wales Faculty of Law

22 September 2006, revised 30 October 2006

Contents

Introduction

This submission is by the following researchers at the Cyberspace Law & Policy Centre <http://www.cyberlawcentre.org/>, University of New South Wales Faculty of Law: Professor Graham Greenleaf and David Vaile (co-directors), Alana Maurushat, Catherine Bond and Abi Paramaguru (postgraduate researchers). The Centre's focus is on research into networked transactions from a public interest perspective.

The authors are involved in the 'Unlocking IP' project, an ARC-funded project which examines the protection and expansion of Australia's information commons[1]. Other investigators in the project have not been involved in the preparation of this submission.

An earlier submission was made in relation to the Exposure Draft. This submission modifies our submissions where changes in the text warrant this, and it otherwise mirrors the earlier submission.

Criticism of the general approach

Our general approach is that we consider that the approach taken to Technological Protection Measure (TPM) protection in the current provisions, the Australia-US Free Trade Agreement, and the proposed amendments are all undesirably broad. Aspects of the provisions that in our view are not in the public interest include:

- that they do not allow for exemptions for circumventions for the purposes of exercising fair dealing rights, or
- to access materials not protected by copyright, or
- for other uses allowed by law.

Furthermore, some supply of circumvention devices for these purposes should be allowed.

However, rather than these issues of broader principle, the focus of this submission is restricted to improvements to the current proposals that are feasible, given that the amendments to copyright law required by the Australia-US Free Trade Agreement (FTA) makes the continuation or alteration of certain aspects of TPM law now unavoidable.

Support for certain provisions

There are a number of aspect of the draft Bill which we wish to support as improvements on the current legislation. We note them here, we do not discuss these in detail later.

- The overall attempt to ensure that TPMs must be connected with copyright infringement is supported strongly, but we make suggestions for improvement
- The proposed action for groundless threats of legal proceedings (s202A) is highly desirable because of the potential these provisions have to be misused to deter legitimate research and to support otherwise anti-competitive conduct.
- The limiting of criminal liability only to cases where a person engages in the conduct for the purpose of "commercial advantage or profit."

[1] See <http://www.cyberlawcentre.org/unlocking-ip/> and particularly the Background Paper contained there.

- The exception relating to interoperability is necessary from a competition and consumer perspective, and will help to reduce barriers to entry to various markets.

- In general, the proposed exemptions are desirable, but deserve to be strengthened.

Undesirable breadth of definitions of TPM and circumvention

Removal of 'effective' from the definition of TPM

In our view, the definition of 'technological protection measure' in s10(1) is inconsistent with the FTA, the WIPO Copyright Treaty (WCT), the WIPO Performances and Phonograms Treaty (WPPT), and Australian case law.

FTA: Section 17.1.4.7(b) explicitly defines an "*effective* technological measure" keeping with the language utilized by the WCT and WPPT. The definition under the current draft bill excludes "effective." This is a derogation from the FTA, WCT and WPPT. We further note that the FTA section does not adequately define what is meant by the word "effective". Any definition of "effective technological measure" in the *Copyright Act* should do so. Our suggested wording is found in our submission below.

WCT and WPPT: Article 11 WCT and Article 18 WPPT mandate that legal protection of *effective* technological measures. There have been many suggestions by experts as to the meaning of "effective" in this context. One relatively uncontroversial conclusion that can be drawn is that *not every* TPM is subject to legal protection. This supposition is supported in the wording of the FTA as well as in Australian case law.

Australian case law: The original definition of "technological protection measure" in s10 of the *Copyright Act 1968* did not include the term "effective." The definition of "circumvention device", however, specifically referred to "an effective technological protection measure." The issue of what constituted an "effective technological protection measure" became one of the main issues in the decisions leading up to the High Court of Australia decision in *Stevens v Kabushiki Kaisha Sony Computer Entertainment* [2005] HCA 58. Prior to the appeals at the Federal Court and later the High Court of Australia, the word "effective" was removed from the definition of 'circumvention device' by the *Copyright Amendment (Parallel Importation) Act 2003.* While the two appeals did not deal specifically with the notion of "effective", the High Court made specific references to the rejection of the definition suggested by the Australian Parliamentary Committee by the International Intellectual Property Alliance (IPA), which definition mirrored the provision in the United States in the *Digital Millennium Copyright Act of 1998* (DMCA). In the AUSFTA, however, Australia has explicitly adopted the wording as proposed by IPA and as reflected in the DMCA. The FTA wording, as noted above, specifically refers to *effective technological measure*.

Importance of re-affirming that TPMs must be 'effective'

The removal of the term *effective technological protection measure* from the definition of *technological protection measure* and *circumvention device* in the earlier draft may have unintended consequences:

- It would expand the scope of protection to weak and often ineffective technologies which should not be given legal protection. These would include: passwords, basic cipher/'rot' technologies (i.e., the mere shifting of letters, eg. a=c, d=f), exclusive technologies (i.e., white coloured "H" with black background becomes a black

coloured "H" with white background) – all basic encryption technologies known since the 9th Century.

This example is not merely whimsical. The criminal charges brought under the DMCA (later dismissed) against Russian computer scientist, Dmitri Sklyarov, involved his circumventing such 9th Century techniques (exclusive and rot encryption technologies).

- It allows for a host of potentially abusive litigation. The United States has had cases of TPMs involving cell phones, printer cartridges and garage door openers. These cases were not about copyright (and in certain instances were rightfully dismissed as such) but involved anti-competitive practices to gain advantage in the market. While it is likely that the Australian courts would dismiss such legal actions as they are clearly an abrogation from the principles in the *Copyright Act*, the damage would have already been done. As prominent Internet analyst Michael Geist notes, "the mere threat of a lawsuit is frequently enough to dissuade many companies from entering the market or from developing an innovation new product." [2].

- Unlike in the United States, the Australian courts have not adopted the principle of 'copyright misuse'. This equitable defence in American law is applicable to cases of infringement where the plaintiff's actions expand copyright beyond the limits imposed by copyright law (eg. anti-competitive acts). It is therefore essential for Australian legislation to deter inappropriate and abusive litigation.

[NB: We note that while the word 'effective' has not been inserted into the new definition as we earlier submitted, the new wording does now refer simply to 'controls' or 'restricts' (rather than 'is intended to control' or 'is designed to restrict'). This may well be read to imply such an 'effectiveness' qualification - it appears to apply to the case where a device actually has such an effect, not merely where it is described as intended to have such an effect. If this is the intention then it is also welcome, and a substantial improvement.

However remain good reasons to require explicit reference to the "effective" test, not least because this is a significant aspect of the FTA text. So we re-present the submission.]

The definition needs to be amended to restore 'effectiveness' as an element of a TPM.

> **Submission 1:** Section 10(1) should be amended to become a definition of an '*effective* technological protection measure' and its wording should be altered so that (b) refers to '*effectively* prevent or inhibit the doing on an act' [3].

---

[2] M Geist, '30 Days of DRM' at <http://www.michaelgeist.ca/daysofdrm>

[3] In other words we suggest a change to "Repeal the definition, substitute:
effective technological protection measure means an device, product or component (including a computer program) that:
(a)is used by, with the permission of, or on behalf of, the owner or the exclusive licensee of the copyright in a work or other subject-matter; and
(b) is designed, in the normal course of its operation, to **effectively** prevent or inhibit the doing on an act:
(i) that is comprised in the copyright; and
(ii) that would infringe the copyright"

Access control technological protection measures should be 'effective'
The definition of 'access control technological protection measure' (ACTPM) has the same deficiency. Please refer to suggestions and arguments as presented in the above section on definition of *effective technological protection measure*.

> **Submission 2:** Definition of 'access control technological protection measure' in subsection 10(1) should be amended to reflect the proposed wording change in the definition of technological protection measure, above.

Market segmentation
Our earlier concerns (in our original submissions 3 and 4) were that the proposed wording of the original Note designed to exclude market segmentation may not have achieved its intended goal because Technological Protection Measures, specifically those which utilize computer programs, are often developed for multiple purposes, and the computer code used in the program is often not set out in a manner which would allow someone to separate the market segmentation components from other components. For example, the TPM used in computer game consoles performs two distinct functions: (1) enforce region coding/market segmentation, and (2) prevent unauthorized games from playing on its console. These two functions may be separated but the computer code performing these functions may be inseparable. We said then that 'the proposed wording of "solely designed to control market segmentation" would allow a company to design a TPM with multiple functions in order to continue to utilize market segmentation.'

The originally proposed test ("solely designed to control segmentation") and the Note itself have been omitted in favour of the construction that an ACTPM "does not include [such devices] to the extent that... " they meet the new exclusions in new paragraphs (c), geographic market segmentation, and (d), restrictions on the use of other goods and services.

To the extent that this removes the anomaly we identified in our earlier submission 4 (that few ACTPMs would be 'solely' aimed at, eg, region encoding) we welcome this change. It removes some of the problems we envisaged.

However, while conceptually it is possible to conceive of an exclusion to a provision applying *'to the extent that'* the relevant device etc. controls or restricts action as described, in practise there may be new practical difficulties introduced by this qualifier, in the cases where many functions are integrally embedded in the one algorithm or computer software module. It may not be possible to disentangle the permissible function from that in (c) or (d).

> **Submission 3:** The wording related to market segmentation in the definitions of *access control technological protection measure* and *technological protection measure* should be reviewed to explicitly cover the situation of a device with both permissible (copyright TPM) and non-permissible (eg region or product restrictions) purposes.

> **Submission 4:** In the definition of '*access control technological protection measure'* and '*technological protection measure', insert 'effective' where appropriate*

Undesirable breadth of definition of circumvention
Section 116AN(1) defines the action for the act of circumvention of an ACTPM, though 'circumvention' remains undefined. If a person does an act which circumvents an ACTPM

without causing any breach of copyright (for example, if they only do so in order to reproduce a work which is in the public domain, or to exercise a right of fair dealing), then there is no good policy reason why such circumvention should be prohibited.

The AUSFTA cl 7(a)(i) refers to TPMs that copyright owners 'use in connection with the exercise of their rights and that restrict unauthorised acts in respect of their works' and that circumvent a TPM that controls access to a protected work. Where an act of circumvention does not result in a breach of an owner's copyright cl 7 could be interpreted to only apply where an actual circumvention results.

> **Submission** 5: Concerning the meaning of circumvention, s116AN(1) should have added a clause (c) "and the act results in a breach of copyright in the work or other subject matter by the person or another person".

Without such an addition the attempt to limit protection of TPMs to those situations connected with copyright protection will be ineffective.

Need to strengthen exceptions

We consider all of the following exceptions to be desirable, but requiring some improvement. The inclusion of specific exceptions, especially those which involve functions related to the computer science community, is very desirable.

The comments below reflect a combined reading each of the interoperability sections (circumvention of an access control TPM, manufacturing of a circumvention device, and circumvention service). Suggestions are, however, only put forth for in the first instance, circumvention of an access control TPM.

Permission exception

We strongly support this exception, in particular the 'reasonable grounds' test, which will avoid accidental infringement where a person was acting in good faith on the belief of permission. However, it should also apply to those activities where at present it is not mentioned, such as manufacturing or providing a circumvention device. For example, the owner should be able to give effective permission to a third party to manufacture or provide a circumvention device, which manufacture or provision would under the draft be not permitted even though the use of the device or service would be.

> **Submission 6:** The Permission exception should also apply to those activities where at present it is not mentioned, such as ss.116AO and ss.116AP, manufacturing or providing a circumvention device.

Interoperability exception

The limitation of the interoperability exception for only access control TPMs, and not TPMs generally, is problematic for a number of reasons:

- **Access control and copy control TPMs may be difficult to categorize**. TPMs very often display both access control and use control characteristics. Where TPMs have both access and copy characteristics, the adoption of a legal exception that only authorizes one form will inevitably lead to more confusion than clarity in its practical application. For example, a prevalent form of copy control technology is a digital rights management system (DRM). DRMS often incorporate TPMs in their applications. A DRM consists of two components: a database containing information

which identifies the content and rightsholders of a work, and a licensing arrangement which establishes the terms of use for the underlying work. DRMs often include digital rights language software such as XrML. Technologies such as XrML have the ability to set licensing terms and the technological capability of controlling both the use of and access to a work well beyond the boundaries of the copyright regime. The interoperability exception solely authorizing circumvention of access control measures becomes inapplicable.

- **Exceptions may be rendered void by licensing provisions.** The current amendments to the *Copyright Act* pose confusion in the area of fair dealings defences and the exceptions to the circumvention of technological protection measures. It is unclear as to whether licensing provisions may lawfully prohibit exceptions to the circumvention of TPMs. This type of approach should be strongly avoided. Clarification may be required in the Act on this point.

Concerning the offences created under section 132APC, as previous discussed, TPMs often display access and copy functions; they are difficult to categorize. It therefore seems illogical that a person would only commit an offence where an access control TPM has been circumvented.

Interoperability relates not only to computer programs but also to devices, products, and components. Please refer to section on exception – computer security testing.

> **Submission 7:** Concerning interoperability, amend "access control technological measure" to "technological protection measure" as paralleled in the manufacturing of devices and circumvention sections in s116AN(3)(a).
>
> **Submission 8:** Concerning interoperability, amend "access control technological measure" in ss.132APC (1)(c) and 132APC (3)(a) to "technological protection measure."
>
> **Submission 9:** Amend "a copy of a computer program (the original program)" to "a device, product, component or computer program (the original program)" in each of ss. 116AN (3)(b)(i) and 132APC (3)(b)(i).

Encryption research exception

Please refer to above arguments for interoperability exception.

> **Submission 10:** Amend "access control technological measure" to "technological protection measure" as paralleled in the manufacturing of devices and circumvention sections in s.116AN (4).
>
> **Submission 11:** Amend "access control technological measure" in s132APE (4)(a) to "technological protection measure."

Computer security testing exception

Please refer to above arguments for interoperability exception.

The computer security testing as presently worded only includes acts related to copies of a computer program. No harm could be done by broadening the exception to include devices, products, and component. This is perhaps best illustrated by way of example. Many USB devices (memory sticks) now incorporate finger print identification technology. A variety

of information may be stored on USB devices from personal information to photographs and works protected by copyright. The finger print identification function would be considered an access control TPM. The ability to perform security testing on this device would be imperative. The current wording of the exception may prevent such types of testing.

> **Submission 12:** Concerning computer security testing, amend "access control technological measure" to "technological protection measure" as paralleled in the manufacturing of devices and circumvention sections in s.116AN(5)(a).
>
> **Submission 13:** Concerning computer security testing, amend "a copy of a computer program (the original program)" to "a device, product, component or computer program (the original program)" in s.116AN(5)(b)(i).
>
> **Submission 14:** Concerning computer security testing, amend "a copy of a computer program (the original program)" to "a device, product, component or computer program (the original program)" in s.132APC(5)(b)(i).

Online privacy exception

The exception for online privacy, while commendable in sentiment, will not as presently drafted be effective to protect privacy as is required by Australian law. The problem is that the proposed exception only allows self-defence against a TPM where it has an 'undisclosed capability' to collect or disseminate personally identifying information.

In contrast, the *Privacy Act 1988*'s National Privacy Principles will in some situation make mere disclosure of 'capability' (whatever that means) insufficient for compliance with the Act. Excessive, unlawful, unfair or unreasonably intrusive collection of personal information will breach the Act (NPPs 1.1, 1.2). Collection without the provision of the required statutory notice (NPP 1.3 items (a)-(f)) will also breach the Act. These deficiencies, where they apply because of the collection of personal information, cannot be cured by a TPM having a 'disclosed capacity'. Similarly, where a TPM discloses personal information that it collects to some other person, there may easily be a breach of NPP 2, and once again it may not be cured by disclosure of the TPM's 'capacity'. Under some circumstances there may be further breaches if personal information is transferred overseas (NPP 9, 'Transborder data flows'). In summary, Australian law does not allow a breach of privacy law to be avoided by announcing an intention to do so.

It is not uncommon (though not universal) for TPMs to collect personal information about users of works (NPP 1), and to transfer that information (via Internet) to the owner of the copyright work or their representative (NPP 2), including in cases where the recipient may be overseas (NPP 9). Questions may also arise about the adequacy of the security of the information (NPP 4). Particularly in cases where the recipient of the information may be overseas and any attempts to obtain remedies through the Australian Privacy Commissioner or the Courts may be futile, Australian consumers need to have some means of self-defence against privacy-invasive TPMs.

> **Submission 15:** There should be added an additional exception to s.116AN, "Subsection (1) does not apply if the person using the access control technological protection measure uses it in a way which breaches the *Privacy Act 1988*."

Alternatively, the exception discussed below under 'An additional exception for breaches of Australian law' would have the same effect.

Law enforcement and national security exception
We support this exception but think the logic behind it should be extended, as noted below under 'An additional exception for breaches of Australian law'.

Libraries exception
We support this exception but consider that additional exceptions in relation to libraries and archives are needed.

Prescribed acts – Exceptions by regulations
The Bill allows the Minister to recommend to the Governor-General that additional prescribed acts appear in the Regulations if a submission is made to the Minister and fulfils the elements of section 249(4). Section 249(5) states that if the Minister receives such a submission, a recommendation must be made "as soon as practicable after receiving the submission, but in any case, within four years of receiving it".

This provision does not fully reflect what the AUSFTA allows. Article 17.4.7(e)(viii) of the AUSFTA states the an exception may be made for "non-infringing uses of a work…when an actual or likely adverse impact on those non-infringing uses is credibly demonstrated in a legislative or administrative review or proceeding; provided that any such review or proceeding is conducted at least once every four years from the date of conclusion of such review or proceeding."

This issue was dealt with in Chapter 5 of the House of Representatives Standing Committee on Legal and Constitutional Affairs Review of Technological Protection Measures Exceptions. The Committee recommended the Attorney General's Department conduct "a statutorily defined, public administrative review" (Recommendation 36).

In our view, while it is desirable that the Minister should be able to respond quickly with an exemption by regulation when a need is demonstrated, section 249 should also explicitly allow for Parliamentary consideration of exceptions at least every four years, including a calling for submissions from the public regarding possible new exceptions, resulting in recommendations to the Minister. Such a periodic public review will allow the TPM legislation and the exceptions to better suit the changing requirements of society and technology.

> **Submission 16:** Section 249 should include a clause explicitly stating that a Parliamentary review of the exceptions to circumvention of a technological protection measures must occur at least every four years, as allowed under the terms of the AUSFTA.

Suggested additional exceptions

We appreciate that the FTA sets out a procedure by which additional exceptions may be created. As noted above, we think the legislative implementation of this procedure could be approved. We consider that the first additional exception that we suggest below (re breaches of Australian law) should be included in the legislation now. The other exceptions suggested would be appropriate for implementation by subsequent regulations and compliance with FTA procedures.

An additional exception for breaches of Australian law
A TPM should not obtain legal protection where its operation results in a breach of Australian law. The new limitation on the definition of TPMs to exclude market

segmentation devices recognises that TPMs should not be allowed to breach trade practices laws. The exception for law enforcement, national security and other government functions recognises that public agencies should have the right to circumvent TPMs wherever they do so in order to carry out their legal duties. The revisions to the privacy exemption proposed above are based on the same principle.

It would clearly be good policy, and consistent with these examples, to also have a general exemption from protection wherever the operation of a TPM is in breach of Australian law. It is impossible to anticipate all situations where such breaches of the law by use of a TPM may occur. A person against whom action is taken for circumvention of a TPM should be able to raise the illegality of that TPM's use as a defence to the alleged act of circumvention. In the circumstances suggested, this constitutes self-defence against an illegal act. The person raising the defence will have the onus of proof of the illegality.

There is no reason why the FTA should reward breaches of Australian law with legal protection for the TPM instrumental in the breach. The FTA does not need to explicitly recognise such an exception, but in any event such a limitation can be read as implied by the FTA in a number of ways. Clause 7(b) refers to an 'effective' TPM, and to one which 'in the normal course of its operation' controls access or protects copyright. A TPM is not 'effective' if it requires illegal means to achieve effectiveness, and a 'normal course of operations' should not involve illegal acts.

> **Submission 17:** There should be added an additional exception to s116AN, "Subsection (1) does not apply if the person using the access control technological protection measure uses it for a purpose which is in breach of Australian law."

An additional exception for orphan works

"Orphan works" are works where it is impossible for a potential user to contact the owner to ask permission to undertake certain acts in relation to the work. Unless potential users are willing to breach copyright in the work, it remains unused or underused until it is enters the public domain through expiry of the duration of copyright (and there may be difficulties in calculating when that occurs).

The proposed Bill would further exacerbate the problem of orphan works. If a TPM is applied to a work and the work subsequently becomes an 'orphan', the public will be unable to utilise the work, even if there is created a copyright exception in relation to orphan works. There will be no way for the public to legitimately circumvent the TPM in order to access the underlying, abandoned work if permission cannot be sought from the copyright owner. However, under these circumstances there is no reason to assume that the copyright owner wishes the TPM protection to continue, since they have abandoned the work itself.

The proposed *Copyright Amendment Regulations 2006* provide an exception for libraries to circumvent a TPM in order to reproduce or communicate a part of the whole of an article or published work to a person for research or study, pursuant to section 49 of the existing *Copyright Act*, which may sometimes be relevant here. However, there needs to be an assurance that ordinary usage of the work can be guaranteed beyond this limited exception.

The Legal and Constitutional Affairs in its *Review of Technological Protection Measures Exceptions* said "the Committee would also support any moves to render the use of 'orphaned' works non-infringing". In our view the Act should explicitly deal with this issue as soon as possible. The absence of such a provision could have a significantly detrimental

impact on the development of the information commons, with the impact being irreversible if the issue is not dealt with appropriately. While it is understandable that the Government may be apprehensive about introducing a broad exception allowing the public to circumvent a TPM in these circumstances, a broader exception permitting libraries, archives and educational institutions to do so is preferable. Although there is no specific provision identifying this issue in the AUSFTA, Article 17.4.7(e)(viii) is sufficiently broad to permit this exception, given the "actual or likely impact on non-infringing uses" that these problems may have.

> **Submission 18:** If the government addresses the need for an exception to copyright infringement in relation to orphan works (as we think it should), then it should also address by regulation the need for an exception allowing circumvention of TPMs which protect them.

An additional exception for orphan TPMs

A second issue arises in relation to potential 'orphan' TPMs. Recommendation 18 of the House of Representatives Standing Committee on Legal and Constitutional Affairs in its *Review of Technological Protection Measures Exceptions* stated that if the "tinkering, decompilation and exploitation of 'abandonware' " becomes non-infringing, a TPM exception should accordingly be created. We agree, but note that TPMs are themselves capable of becoming 'abandonware'. Such 'orphan TPMs' do not come under the "malfunctioning technological protection measures" exception provided in the *Copyright Amendment Regulations 2006*, so a separate exception will be needed.

There are good reasons to allow circumvention of such 'orphan TPMs'. The extent to which the proposed amendments will protect TPMs used by third parties (persons other than the owner of the work or persons acting on the owner's behalf) to restrict access to a work is somewhat uncertain. But to the extent that that they do, then it may be difficult or impossible for anyone to obtain access to such works, whether they have the consent of the copyright owner or whether they have some other legitimate reason to access the work. In such cases where a person has a right to use a work, and the TPM has not been used on behalf of the copyright owner, there should be a right to circumvent it.

> **Submission 19:** Whether or not the Government creates an exception for 'abandonware' (as we think it should), it should introduce an additional exception that explicitly allows a person who has a right to use a work to circumvent an orphan TPM, where that TPM has not been used by or on behalf of the owner of copyright in the work.

Summary of submissions

> **Submission 1:** Section 10(1) should be amended to become a definition of an '*effective* technological protection measure' and its wording should be altered so that (b) refers to '*effectively* prevent or inhibit the doing on an act'.
>
> **Submission 2:** Definition of 'access control technological protection measure' in subsection 10(1) should be amended to reflect the proposed wording change in the definition of effective technological protection measure above.
>
> **Submission 3:** The wording related to market segmentation in the definitions of *access control technological protection measure* and *technological protection*

measure should be reviewed to explicitly cover the situation of a device with both permissible (copyright TPM) and non-permissible (eg region or product restrictions) purposes.

Submission 4: In the definition of '*access control technological protection measure'* and '*technological protection measure'*, insert *'effective'* where appropriate

Submission 5: Concerning the meaning of circumvention, s.116AK (1) should have added a clause (c) "and the act results in a breach of copyright in the work or other subject matter by the person or another person".

Submission 6: The Permission exception should also apply to those activities where at present it is not mentioned, such as ss.116AL and 116AM, manufacturing or providing a circumvention device.

Submission 7: Concerning interoperability, amend "access control technological measure" to "technological protection measure" as paralleled in the manufacturing of devices and circumvention sections in s. 116AK (3)(a).

Submission 8: Concerning interoperability, amend "access control technological measure" in ss.132APA (1)(c) and 132APA (3)(a) to "technological protection measure."

Submission 9: Amend "a copy of a computer program (the original program)" to "a device, product, component or computer program (the original program)" in each of ss.116AK (3)(b)(i) and s.132APA (3)(b)(i).

Submission 10: Amend "access control technological measure" to "technological protection measure" as paralleled in the manufacturing of devices and circumvention sections in s.116AK(4).

Submission 11: Amend "access control technological measure" in s.132APA (4)(a) to "technological protection measure."

Submission 12: Concerning computer security testing, amend "access control technological measure" to "technological protection measure" as paralleled in the manufacturing of devices and circumvention sections in s.116AK(5)(a).

Submission 13: Concerning computer security testing, amend "a copy of a computer program (the original program)" to "a device, product, component or computer program (the original program)" in s.116AK(5)(b)(i).

Submission 14: Concerning computer security testing, amend "a copy of a computer program (the original program)" to "a device, product, component or computer program (the original program)" in s.132APA(5)(b)(i).

Submission 15: There should be added an additional exception to s.116AN, "Subsection (1) does not apply if the person using the access control technological protection measure uses it in a way which breaches the *Privacy Act 1988*."

Submission 16: Section 116AK should include a clause explicitly stating that a Parliamentary review of the exceptions to circumvention of a technological

protection measures must occur at least every four years, as allowed under the terms of the AUSFTA.

Submission 17: There should be added an additional exception to s.116AN, "Subsection (1) does not apply if the person using the access control technological protection measure uses it for a purpose which is in breach of Australian law."

Submission 18: If the government addresses the need for an exception to copyright infringement in relation to orphan works (as we think it should), then it should also address by regulation the need for an exception allowing circumvention of TPMs which protect them.

Submission 19: Whether or not the Government creates an exception for 'abandonware' (as we think it should), it should introduce an additional exception that explicitly allows a person who has a right to use a work to circumvent an orphan TPM, where that TPM has not been used by or on behalf of the owner of copyright in the work.