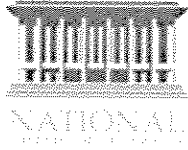


RECEIVED
17 OCT 2006

BY: LACA



Submission No.	28
Date Received	

Parliament of Australia

House of Representatives Standing Committee
on Legal and Constitutional Affairs

Review of Technological Protection Measures Exceptions

National Library of Australia Submission

17 October 2005



17 October 2005

The Secretary
House of Representatives
Standing Committee on Legal and Constitutional Affairs
Parliament House
CANBERRA ACT 2600

CANBERRA ACT 2600 AUSTRALIA

TELEPHONE (02) 6262 1111

HOME PAGE ADDRESS
<http://www.nla.gov.au>

TELEPHONE TYPEWRITER NUMBER
1800 026 372

NATIONAL LIBRARY FACSIMILE
(02) 6257 1703

Dear Ms Towner

The National Library of Australia is pleased to have the opportunity to make a submission to the Review of Technological Protection Measures Exceptions.

The functions of the National Library of Australia (the Library) are set out in the *National Library Act 1960*. Under the *Act* the Library has a mandate to develop a collection of information resources relating to Australia and the Australian people and to make these resources available for use by the public and members of Parliament. The Library also has a mandate under its *Act* to provide leadership to the Australian library sector in matters of national interest. The *Copyright Act 1968* and the *Copyright Amendment (Digital Agenda) Act 2000* assists the Library in its roles of collecting, preservation and provision of access to information.

Significantly, the *Copyright Act* establishes a set of principles which upholds a balance between the rights of creators and authors and the rights of users. The principle of fair dealing is fundamental to safeguarding equity of access to information by all Australians. To support this the *Copyright Act* contains exceptions for libraries and archives which allow them to operate for the public good by:

- copying and lending works in copyright directly to individuals and other libraries to the extent permitted by the *Copyright Act*
- preserving works for access by future generations of Australians

The *Copyright Amendment (Digital Agenda) Act 2000* upholds the principle of fair dealing in the digital environment and at the same time contains a commercial availability test which ensures that copying and lending of works by libraries does not undermine the livelihood of creators, publishers or vendors of digital content.

While the *Digital Agenda Act* introduced 'paracopyright' laws it also extended the exceptions to infringement by way of circumvention in order to maintain a degree of balance. These exceptions allow the Library to perform its functions as illustrated in Appendix 1, and any exceptions that are introduced should continue to uphold the balance that has been struck by the *Digital Agenda Act* and should not prevent the Library from continuing with its functions.

The *Australia-United States Free Trade Agreement 1 January 2005* (AUSFTA) has extended the term of copyright from fifty to seventy years. The Library believes that because of this lengthy extension of the copyright term, it is vitally important that no further legislative changes should be made, or new legislation enacted, that will compromise the ability of the Library to provide access to works under the principle

of fair dealing. If further restrictions and barriers are created by legislation relating to the use of technological protection measures, then public access to information will be significantly eroded. Not only will current public access to information in digital form be jeopardised but future access to information published in digital form will also be at risk if the Library is unable to preserve this material before the software and hardware used for publication becomes obsolescent. This is a problem that is increasing exponentially given the pace of technological change.

The Library understands that there is a requirement to show a 'credibly demonstrated need' to circumvent a technological prevention measure in order to gain access to works that are technically locked up by creators or vendors. The Library submits that it cannot perform its role and functions if it is unable to access technologically protected works for the purposes of preservation and fair dealing and that this is without question a 'credibly demonstrated need'. To assist the Committee's understanding of the Library's role and functions and its management of digital works, I have attached a table of examples of classes of works that the Library collects, preserves and provides public access to under the terms of the *Copyright Act*, and that may be affected by legislative changes relating to technological protection measures. Please note that these examples represent a mixture of current practise and future scenarios. Some examples also illustrate existing barriers to preservation of digital works within the *Copyright Act*.

The Library is concerned that using classes of works for the purpose of exceptions to technological protection measures may adversely affect our ability to preserve and provide access to digital works and is therefore not in the public interest. The rapidly increasing pace of technological change means that many classes of works may evolve and become obsolete within a very short timeframe. It is therefore impractical to use a narrowly defined list of exceptions which will become out-of-date very quickly. The Library suggests that a much broader definition be used to describe exceptions for libraries. This could be as simple as 'digital works'.

As a member of the Australian Libraries Copyright Committee and the Australian Digital Alliance, the Library endorses the submissions of these bodies.

I would be pleased to provide the Committee with further information or to speak to the Committee either in private or through a process of public hearings.

Yours sincerely



Jan Fullerton
Director General

Class of Work	Impact of not allowing circumvention	Example Scenarios
Literary, dramatic, artistic or musical works in digital form, including computer programs, distributed in formats which are protected by copy protection mechanisms. Specific formats: Literary works on magnetic disc Literary works on magnetic tape Literary works on CD Literary works on DVD Literary works on storage devices Literary works online Dramatic works on magnetic disc Dramatic works on magnetic tape Dramatic works on CD Dramatic works on DVD Dramatic works on storage devices Dramatic works online Artistic works on magnetic disc Artistic works on magnetic tape Artistic works on CD Artistic works on DVD Artistic works on storage devices Artistic works online Musical works on magnetic disc Musical works on magnetic tape Musical works on CD Musical works on DVD Musical works on storage devices Musical works online	<ul style="list-style-type: none"> Inability to make copies of works for preservation purposes, especially in advance of media degradation, failure, damage or loss, or in advance of obsolescence of hardware or software required to allow display and use of the works. Inability to make backup copies of computer programs. <p>Comments: The physical carriers (floppy disc, CD, DVD, video tape, memory cards etc.) on which works may be distributed will degrade, become damaged or become obsolete long before the expiration of copyright (perhaps within 5-10 years of creation). These materials need to be transferred to alternative carriers or long-term storage systems for preservation, preferably before they become degraded, damaged or lost.</p> <p>Inability to circumvent copy protection mechanisms on these materials would mean that these works could not be preserved beyond the life of the original medium, or the technology needed to replay it (e.g. floppy disc drives, memory card readers).</p> <ul style="list-style-type: none"> Inability to make copies of works for communication to library, archives or museum users. Inability to make and communicate copies of works in alternative access formats. 	<ul style="list-style-type: none"> A library acquires a multimedia publication which is distributed as an executable computer program on a CD-ROM that is copy-protected. In order to create a backup copy of the computer program, or to create a copy of the publication for preservation purposes, the copy protection mechanism would need to be circumvented. It would be preferable to allow creation of preservation copies prior to the degradation, damage or loss of the publication, as once degradation, damage or loss has occurred, there may no longer be copies available from which preservation copies may be created. Professional audio, video and broadcast equipment, and many computer hardware and software devices contain copy protection creation and circumvention devices as an integral and normal part of device function. Each act of duplication for preservation purposes would entail automatic circumvention of protection mechanisms. A library obtains permission to copy a Web site which contains streaming audiovisual media files. It may be necessary to capture copies of the streaming files as they are streamed or broadcast, even though the files may have been streamed to prevent duplication. A library obtains permission to copy a Web site which includes a file declaring a set of robot exclusion rules designed to prevent Web crawler 'robots' from copying certain pages. The rules would need to be circumvented to obtain the permitted copy of the Web site. A library user requests a copy of a sound recording for which they have copyright permission, but which is protected by a copy protection mechanism. The library would need to circumvent copy protection mechanisms in order to provide the copy. Professional audio, video and broadcast equipment, and many computer hardware and software devices contain copy protection creation and circumvention devices as an

		<p>integral and normal part of device function. Each act of duplication for communicating works to users would entail automatic circumvention of protection mechanisms.</p> <ul style="list-style-type: none"> • A sight-impaired person lawfully downloads the text of a research article guarded with a protection measure. He would like to apply 'text to audio' software to listen to the text (i.e. to shift it to an alternative format for access), but is prevented by the TPM. • The proceedings of a scientific conference distributed on CD-ROM are protected by a copy protection mechanism that prevents duplication. The copy held by a library becomes damaged and a replacement copy is required to be made for preservation purposes (sourced from another library, if such another copy exists). Copy protection mechanisms would need to be circumvented to enable a replacement copy or copy for preservation purposes to be made. If circumvention is not allowed, the conference proceedings would be lost to the library and its users.
<p>Literary, dramatic, artistic or musical works in digital form, including computer programs, where access is protected by encryption technologies (especially where decryption devices or software mechanisms are malfunctioning, damaged, lost or obsolete.)</p>	<ul style="list-style-type: none"> • Inability to make replacement copies of works for other libraries, archives or museums, or for communication to users of other libraries, archives or museums. • Inability to make copies of a reasonable portion of a work for the purposes of research or study • Inability to provide access to original copies of works, preservation copies of works, or copies of works for communication to users. • Inability to reproduce and reverse engineer for interoperability, security testing and error correction. • Inability to reverse engineer for preservation purposes [envisaged]. • Inability to preserve by migrating works to a more modern format, or by emulating on more modern hardware platforms [envisaged]. 	<ul style="list-style-type: none"> • A student downloads the text of an article for research or study purposes which is guarded by a protection measure, but is prevented from copying from the file or emailing the article home, although the intent is for use of the material for the purposes of research or study. • A library acquires the personal papers of a deceased person, among which are personal papers in digital form that are encrypted (either intentionally or unintentionally, as a normal consequence of using a particular software application) and the encryption key or algorithm is not available. In order to preserve and make these materials accessible for users, the library would need to overcome the encryption mechanisms that may be present in the material itself (e.g. encrypted PDF files, or encrypted PST email archives). • A library holds a multimedia publication, the files of which are published in a proprietary, encrypted format. When the supporting hardware and software systems

<p>Literary, dramatic, artistic or musical works in digital form, including computer programs, where access is protected by software keys, passwords or other software authorisation measures, (especially where keys or authorisation measures are malfunctioning, damaged, lost or obsolete.)</p>	<ul style="list-style-type: none"> • Inability to provide access to original copies of works, preservation copies of works, or copies of works for communication to users. 	<p>become obsolete, access to the publication may be entirely lost, unless it can be accessed under emulation, or can be reverse engineered and transferred to another format, which would require the encryption to be circumvented to preserve access.</p> <ul style="list-style-type: none"> • A library acquires the personal papers of a deceased person, among which are personal papers in digital form that are protected by a password, and that password has not been supplied or is unknown or lost. In order to preserve and make these materials accessible for users, the library would need to bypass the password protection mechanisms that may be present in the material itself (e.g. password protected PDF files, or password protected PST email archives). • A library lawfully holds the authorisation key to a software application in its collection, by which it provides limited access to the application to its users. If the library creates a preservation copy of the software application, it must also be able to provide and use the authorisation key to continue to provide access to the preserved application. • In cases where a library needs to migrate materials from obsolete formats or set them up in an archival environment, the password or software protection may need to be disabled or cannot be supported in the new format or operating environment.
<p>Literary, dramatic, artistic or musical works in digital form, where access is protected by specific hardware requirements (e.g. dongles, specific hardware platforms, or requirement for original media or hardware) (especially where such hardware is malfunctioning, damaged, lost or obsolete.)</p>	<ul style="list-style-type: none"> • Inability to make copies of works for preservation purposes, especially in advance of media degradation, failure, damage or loss, or in advance of obsolescence of hardware or software required to allow display and use of the works. • Inability to preserve by migrating works to a more modern format, or by emulating on more modern hardware platforms. • Inability to make copies of works for communication to library, archives or museum users. 	<ul style="list-style-type: none"> • Access to a scientific database in a library's collection is controlled by a hardware dongle, which must be attached to the computer on which the database is installed. The dongle is held by a library, through which it provides limited access to the database. In the near future, the dongle may malfunction, or may be incompatible with future hardware changes and software drivers, closing off access to the database. To provide ongoing access to the database, a library would need to circumvent the requirement for the presence of the hardware dongle. • The required hardware and operating system to support the same database will eventually become obsolete. To

	<ul style="list-style-type: none"> • Inability to make replacement copies of works for other libraries, archives or museums, or for communication to users of other libraries, archives or museums. 	<p>continue to provide access to the database, a library may need to migrate the database to an alternative format, or to provide access to the database under emulation of the original hardware and operating system. In either case, the access control of the dongle may not be supported and would need to be bypassed.</p> <ul style="list-style-type: none"> • Use of a particular software application may only be allowed if it is installed from the original floppy disc medium on which it was supplied, through use of a TPM. The original floppy disc will degrade or become damaged. To provide ongoing access to the software application beyond the limited life of the floppy disc, a library would need to copy the application to stable storage media and to circumvent the mechanism which requires its installation or use from the original floppy disc.
<p>Audiovisual works (including sound recordings, images, motion pictures, and dynamic or interactive media) in digital form, including computer programs, distributed in formats which are protected by copy protection mechanisms.</p>	<ul style="list-style-type: none"> • Inability to make copies of works for preservation purposes, especially in advance of media degradation, failure, damage or loss, or in advance of obsolescence of hardware or software required to allow display and use of the works. • Inability to make backup copies of computer programs. • Inability to make copies of works for communication to library, archives or museum users. • Inability to make replacement copies of works for other libraries, archives or museums, or for communication to users of other libraries, archives or museums. 	<ul style="list-style-type: none"> • A library acquires a video recording of a commercial educational motion picture on video tape and on DVD, both of which are protected by different copy protection mechanisms. In order to preserve the motion picture beyond the life of its carrier medium, it would be necessary to circumvent the copy protection mechanisms and to copy the motion picture to alternative media for preservation purposes. <p>It would be preferable to allow creation of preservation copies prior to the degradation, damage or loss of the publication, as once degradation, damage or loss has occurred, there may no longer be copies available from which preservation copies may be created.</p> <p>It may also be necessary to transfer the motion picture to alternative audiovisual data encoding formats for preservation and/or access purposes.</p> <ul style="list-style-type: none"> • A replacement sound recording on a copy-protected audio CD is requested by another library when their copy is lost. The copy protection mechanism would need to be circumvented in order to enable supply of the replacement copy.

		<ul style="list-style-type: none"> • Professional audio, video and broadcast equipment, and many computer hardware and software devices contain copy protection creation and circumvention devices as an integral and normal part of device function. Each act of duplication for preservation purposes or to communicate works to users or other libraries, archives or museums would entail automatic circumvention of protection mechanisms.
<p>Audiovisual works (including sound recordings, images, motion pictures, and dynamic or interactive media) in digital form, including computer programs, where access is protected by encryption technologies (especially where decryption devices or software mechanisms are malfunctioning, damaged, lost or obsolete).</p>	<ul style="list-style-type: none"> • Inability to provide access to works, preservation copies of works, or copies of works for communication to users. • Inability to reverse engineer for interoperability, security testing and error correction. • Inability to reverse engineer for preservation purposes [envisaged]. • Inability to preserve by migrating works to a more modern format, or by emulating on more modern hardware platforms [envisaged]. 	<ul style="list-style-type: none"> • A library, archive or museum acquires an interactive artwork, some files of which were created in a proprietary, encrypted format. When the supporting hardware and software systems become obsolete, access to the artwork may be entirely lost, unless it can be accessed under emulation, or can be reverse engineered and transferred to another format, which would require the encryption to be circumvented to preserve access. • A library obtains permission to copy a Web site containing audiovisual media files. The media files may require proprietary coder-decoder algorithms (codecs), which may need to be reverse engineered, or devices or software created or employed, to transfer the audiovisual content to alternative formats for preservation.
<p>Audiovisual works (including sound recordings, images, motion pictures, and dynamic or interactive media) in digital form, where access is protected by software keys, passwords or other software authorisation measures (especially where keys or authorisation measures are malfunctioning, damaged, lost or obsolete).</p>	<ul style="list-style-type: none"> • Inability to provide access to works, preservation copies of works, or copies of works for communication to users, or other libraries, archives and museums and their users. 	<ul style="list-style-type: none"> • A library lawfully holds the authorisation key to a multimedia application in its collection, by which it provides limited access to the application to its users. If the library creates a preservation copy of the multimedia application, it must also be able to provide and use the authorisation key to continue to provide access to the preserved application.
<p>Audiovisual works (including sound recordings, images, motion pictures, and dynamic or</p>	<ul style="list-style-type: none"> • Inability to make copies of works for preservation purposes, especially in advance of media degradation, failure, damage or loss, or in advance of obsolescence of 	<ul style="list-style-type: none"> • Use of a particular software application may only be allowed if it is installed from the original CD-ROM medium on which it was supplied, through use of a TPM.

<p>interactive media) in digital form, where access is protected by specific hardware requirements (e.g. dongles, specific hardware platforms, or requirement for original media or hardware)</p> <p>(especially where such hardware is malfunctioning, damaged, lost or obsolete.)</p>	<p>hardware or software required to allow display and use of the works.</p> <ul style="list-style-type: none"> • Inability to preserve by migrating works to a more modern format, or by emulating on more modern hardware platforms. • Inability to make copies of works for communication to library, archives or museum users. • Inability to make replacement copies of works for other libraries, archives or museums, or for communication to users of other libraries, archives or museums. 	<p>The original floppy disc will degrade or become damaged. To provide ongoing access to the software application beyond the limited life of the floppy disc, a library would need to copy the application to stable storage media and to circumvent the mechanism which requires its installation or use from the original floppy disc.</p>
<p>Databases, datasets or geospatial works in digital form, including computer programs, distributed in formats which are protected by copy protection mechanisms.</p>	<ul style="list-style-type: none"> • Inability to make backup copies of computer programs. • Inability to make copies of works for communication to library, archives or museum users. • Inability to make replacement copies of works for other libraries, archives or museums, or for communication to users of other libraries, archives or museums. 	
<p>Databases, datasets or geospatial works in digital form, including computer programs, where access is protected by encryption technologies</p> <p>(especially where decryption devices or software mechanisms are malfunctioning, damaged, lost or obsolete.)</p>	<ul style="list-style-type: none"> • Inability to provide access to works, preservation copies of works, or copies of works for communication to users. • Inability to reverse engineer for interoperability, security testing and error correction. • (Inability to reverse engineer for preservation purposes – proposed.) 	
<p>Databases, datasets or geospatial works in digital form, including computer programs, where access is protected by software keys, passwords or other software</p>	<ul style="list-style-type: none"> • Inability to provide access to works, preservation copies of works, or copies of works for communication to users. 	

<p>authorisation measures (especially where keys or authorisation measures are malfunctioning, damaged, lost or obsolete.)</p>	<p>Databases, datasets or geospatial works in digital form, where access is protected by specific hardware requirements (e.g. dongles, specific hardware platforms, or requirement for original media or hardware)</p> <p>(especially where such hardware is malfunctioning, damaged, lost or obsolete.)</p>	<ul style="list-style-type: none"> • Inability to make copies of works for preservation purposes, especially in advance of media degradation, failure, damage or loss, or in advance of obsolescence of hardware or software required to allow display and use of the works. • Inability to preserve by migrating works to a more modern format, or by emulating on more modern hardware platforms. • Inability to make copies of works for communication to library, archives or museum users. • Inability to make replacement copies of works for other libraries, archives or museums, or for communication to users of other libraries, archives or museums. 	<ul style="list-style-type: none"> • Access to a scientific database in a library's collection is controlled by a hardware dongle, which must be attached to the computer on which the database is installed. The dongle is held by a library, through which it provides limited access to the database. In the near future, the dongle may malfunction, or may be incompatible with future hardware changes and software drivers, closing off access to the database. To provide ongoing access to the database, a library would need to circumvent the requirement for the presence of the hardware dongle. • The required hardware and operating system to support the same database will eventually become obsolete. To continue to provide access to the database, a library may need to migrate the database to an alternative format, or to provide access to the database under emulation of the original hardware and operating system. In either case, the access control of the dongle may not be supported and would need to be bypassed.
<p>Literary, dramatic, artistic or musical works, audiovisual works (including sound recordings, images, motion pictures and dynamic or interactive media), databases, datasets or geospatial works in digital form, including computer programs, encoded in proprietary data formats.</p>	<ul style="list-style-type: none"> • Inability to reverse engineer, allow display or use through emulation or viewing applications, or transform to alternative formats for preservation or communication purposes using software or devices which have been developed through reverse engineering of proprietary formats. 	<ul style="list-style-type: none"> • A library acquires the personal correspondence of a depositor in the form of an email archive, which has been stored in a proprietary PST email archive file. In order to preserve and provide access to the correspondence, the library would need to employ software or devices possibly derived from reverse engineering of proprietary formats to view, extract or transform the content into alternative formats for preservation. • Online media files may have proprietary coder-decoder algorithms (codecs), which may need to be reverse engineered, or devices or software created or employed, to transfer the audiovisual content to alternative formats for preservation. E.g. for preservation of Microsoft ASF files. 	