



## EFF ANALYSIS OF THE TPM PROVISIONS IN THE U.S. FEBRUARY 2011 PROPOSAL FOR THE TPP INTELLECTUAL PROPERTY CHAPTER

### Text of Article 4.9 of the U.S. Intellectual Property chapter proposal

9. (a) In order to provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures<sup>i</sup> that authors, performers, and producers of phonograms use in connection with the exercise of their rights and that restrict unauthorized acts in respect of their works, performances, and phonograms, each Party shall provide that<sup>ii</sup> any person who:
- (i) circumvents without authority any effective technological measure that controls access to a protected work, performance, phonogram, or other subject matter;<sup>iii</sup> or
  - (ii) manufactures, imports, distributes, offers to the public, provides, or otherwise traffics in devices, products, or components, or offers to the public or provides services,<sup>iv</sup> that:
    - (A) are promoted, advertised, or marketed by that person, or by another person acting in concert with that person and with that person's knowledge, for the purpose of circumvention of any effective technological measure,
    - (B) have only a limited commercially significant purpose or use other than to circumvent any effective technological measure, or
    - (C) are primarily designed, produced, or performed for the purpose of enabling or facilitating the circumvention of any effective technological measure,

shall be liable and subject to the remedies set out in Article [12.12]. Each Party shall provide for criminal procedures and penalties<sup>v</sup> to be applied when any person, other than a nonprofit library, archive, educational institution, or public noncommercial broadcasting entity, is found to have engaged willfully and for purposes of commercial advantage or private financial gain in any of the foregoing activities. Such criminal procedures and penalties shall include the application to such activities of the remedies and authorities listed in subparagraphs (a), (b), and (f) of Article [15.5] as applicable to infringements, *mutatis mutandis*.<sup>12</sup>

---

**FN 12** For purposes of greater certainty, no Party is required to impose liability under Articles 9 and 10 for actions taken by a Party or a third party acting with the authorization or consent of a Party

- (b) In implementing subparagraph (a), no Party shall be obligated to require that the design of, or the design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure, so long as the product does not otherwise violate any measures implementing subparagraph (a).
- (c) Each Party shall provide that a violation of a measure implementing this paragraph is a separate cause of action, independent of any infringement that might occur under the Party's law on copyright and related rights.<sup>vi</sup>
- (d) Each Party shall confine exceptions and limitations to measures implementing subparagraph (a) to the following activities, which shall be applied to relevant measures in accordance with subparagraph (e):
  - (i) noninfringing reverse engineering activities with regard to a lawfully obtained copy of a computer program, carried out in good faith with respect to particular elements of that computer program that have not been readily available to the person engaged in those activities, for the sole purpose of achieving interoperability of an independently created computer program with other programs;
  - (ii) noninfringing good faith activities, carried out by an appropriately qualified researcher who has lawfully obtained a copy, unfixed performance, or display of a work, performance, or phonogram and who has made a good faith effort to obtain authorization for such activities, to the extent necessary for the sole purpose of research consisting of identifying and analyzing flaws and vulnerabilities of technologies for scrambling and descrambling of information;
  - (iii) the inclusion of a component or part for the sole purpose of preventing the access of minors to inappropriate online content in a technology, product, service, or device that itself is not prohibited under the measures implementing subparagraph (a)(ii);
  - (iv) noninfringing good faith activities that are authorized by the owner of a computer, computer system, or computer network for the sole purpose of testing, investigating, or correcting the security of that computer, computer system, or computer network;
  - (v) noninfringing activities for the sole purpose of identifying and disabling a capability to carry out undisclosed collection or dissemination of personally identifying information reflecting the online activities of a natural person in a way that has no other effect on the ability of any person to gain access to any work;

- (vi) lawfully authorized activities carried out by government employees, agents, or contractors for the purpose of law enforcement, intelligence, essential security, or similar governmental purposes;
  - (vii) access by a nonprofit library, archive, or educational institution to a work, performance, or phonogram not otherwise available to it, for the sole purpose of making acquisition decisions; and
  - (viii) noninfringing uses of a work, performance, or phonogram in a particular class of works, performances, or phonograms when an actual or likely adverse impact on those noninfringing uses is demonstrated in a legislative or administrative proceeding<sup>vii</sup> by substantial evidence; provided that any limitation or exception adopted in reliance upon this clause shall have effect for a renewable period of not more than three years from the date of conclusion of such proceeding.
- (e) The exceptions and limitations to measures implementing subparagraph (a) for the activities set forth in subparagraph [4.9(d)] may only be applied as follows, and only to the extent that they do not impair the adequacy of legal protection or the effectiveness of legal remedies against the circumvention of effective technological measures:
- (i) Measures implementing subparagraph (a)(i) may be subject to exceptions and limitations with respect to each activity set forth in subparagraph (d).
  - (ii) Measures implementing subparagraph (a)(ii), as they apply to effective technological measures that control access to a work, performance, or phonogram, may be subject to exceptions and limitations with respect to activities set forth in subparagraph (d)(i), (ii), (iii), (iv), and (vi).
  - (iii) Measures implementing subparagraph (a)(ii), as they apply to effective technological measures that protect any copyright or any rights related to copyright, may be subject to exceptions and limitations with respect to activities set forth in subparagraph (d)(i) and (vi).
- (f) **Effective technological measure** means any technology, device, or component that, in the normal course of its operation, controls access to a protected work, performance, phonogram, or other protected subject matter, or protects any copyright<sup>viii</sup> or any rights related to copyright.<sup>ix</sup>

### **Text of Article 12.12**

12. In civil judicial proceedings concerning the acts described in Article 4.[9] (TPMs) and Article 4.[10] (RMI), each Party shall provide that its judicial authorities shall, at the least, have the authority to:
  - (a) impose provisional measures, including seizure of devices and products suspected of being involved in the prohibited activity;
  - (b) provide an opportunity for the right holder to elect between actual damages it suffered (plus any profits attributable to the prohibited activity not taken into account in computing those damages) or pre-established damages;<sup>x</sup>
  - (c) order payment to the prevailing right holder at the conclusion of civil judicial proceedings of court costs and fees, and reasonable attorney's fees, by the party engaged in the prohibited conduct;<sup>xi</sup> and
  - (d) order the destruction of devices and products found to be involved in the prohibited activity.

No Party shall make damages available under this paragraph against a nonprofit library, archives, educational institution, or public noncommercial broadcasting entity that sustains the burden of proving that such entity was not aware and had no reason to believe that its acts constituted a prohibited activity.

### **Text of Article 15.5**

5. With respect to the offences described in Article 15.[1]-[4] above, each Party shall provide:
  - (a) penalties that include sentences of imprisonment as well as monetary fines sufficiently high to provide a deterrent to future infringements, consistent with a policy of removing the infringer's monetary incentive. Each Party shall further establish policies or guidelines that encourage judicial authorities to impose those penalties at levels sufficient to provide a deterrent to future infringements, including the imposition of actual terms of imprisonment when criminal infringement is undertaken for commercial advantage or private financial gain;
  - (b) that its judicial authorities shall have the authority to order the seizure of suspected counterfeit or pirated goods, any related materials and implements used in the commission of the offense, any assets traceable to the infringing

activity, and any documentary evidence relevant to the offense. Each Party shall provide that items that are subject to seizure pursuant to any such judicial order need not be individually identified so long as they fall within general categories specified in the order;

- (c) that its judicial authorities shall have the authority to order, among other measures, the forfeiture of any assets traceable to the infringing activity, and shall order such forfeiture at least in cases of trademark counterfeiting;
- (d) that its judicial authorities shall, except in exceptional cases, order
  - (i) the forfeiture and destruction of all counterfeit or pirated goods, and any articles consisting of a counterfeit mark; and
  - (ii) the forfeiture or destruction of materials and implements that have been used in the creation of pirated or counterfeit goods.

Each Party shall further provide that forfeiture and destruction under this subparagraph and subparagraph (c) shall occur without compensation of any kind to the defendant;

- (e) that its judicial authorities have the authority to order the seizure or forfeiture of assets the value of which corresponds to that of the assets derived from, or obtained directly or indirectly through, the infringing activity.
- (f) that, in criminal cases, its judicial or other competent authorities shall keep an inventory of goods and other material proposed to be destroyed, and shall have the authority temporarily to exempt such materials from the destruction order to facilitate the preservation of evidence upon notice by the right holder that it wishes to bring a civil or administrative case for damages<sup>28</sup>; and
- (g) that its authorities may initiate legal action *ex officio* with respect to the offenses described in this Chapter, without the need for a formal complaint by a private party or right holder.

---

FN 27

For purposes of this Article, “illicit label” means a genuine certificate, licensing document, registration card, or similar labeling component:

- (A) that is used by the copyright owner to verify that a phonogram, a copy of a computer program or literary work, a copy of a motion picture or other audiovisual work, or documentation or packaging for such phonogram or copies is not counterfeit or infringing of any copyright; and
- (B) that is, without the authorization of the copyright owner— (i) distributed or intended for distribution not in connection with the phonogram or copies to which such labeling component was intended to be affixed by the respective

copyright owner; or (ii) in connection with a genuine certificate or licensing document, knowingly falsified in order to designate a higher number of licensed users or copies than authorized by the copyright owner, unless that certificate or document is used by the copyright owner solely for the purpose of monitoring or tracking the copyright owner's distribution channel and not for the purpose of verifying that a copy or phonogram is noninfringing.

FN 28 For greater certainty, a notice from the right holder that it wishes to bring a civil or administrative case for damages is not the sole basis for the authority to exempt materials from the destruction order.

---

## <sup>i</sup> Context

A key part of the United States' intellectual property trade agenda is securing legal protection against circumvention of technological measures added to copyrighted works, based on the provisions in the U.S. Digital Millennium Copyright Act of 1998 (DMCA). Anti-circumvention provisions based on those in the DMCA have been included in the IP chapters of the last 10 bilateral or regional free trade agreements (FTAs) that the U.S. has concluded.

### **International Standard**

This provision implements obligations contained in Article 11 of the 1996 WIPO Copyright Treaty (WCT) and Article 18 of the WIPO Performances and Phonograms Treaty (WPPT). However, while the WCT and WPPT provisions leave considerable discretion to signatory countries on how they implement these obligations, this provision is modeled on the U.S. technological protection measures (TPM) law, the 1998 Digital Millennium Copyright Act.

Article 11 of the WCT provides that:

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

The US TPM provisions are located in sections 1201-1204 of the U.S. Copyright statute: <http://www.copyright.gov/title17/92chap12.pdf>

### **Issues Raised**

Countries' policy choices about the scope and structure of legal protection obligations for TPMs can have significant adverse consequences on national public policy interests outside of the copyright sphere.

As the U.S. experience with the similar provisions in the DMCA over the last 12 years has demonstrated, overbroad legal protection for TPMs has restricted fair use and other lawful uses of copyrighted material for education and a variety of socially beneficial purposes, chilled scientific research and progress in computer security, impeded legitimate competition, and stifled innovation. In particular, overbroad implementation of the WCT and WPPT TPM provisions can:

- 
- Reduce access to knowledge by restricting citizens' lawful non-infringing uses and overriding exceptions and limitations in national copyright law that are used by educators, students, libraries and archives, researchers, scholars, the visually impaired, and others;
  - Result in anti-competitive misuse of TPMs; and
  - Impede technological innovation and the creation of interoperable devices, information tools and technologies, particularly free and open source software.

See *Unintended Consequences: Twelve Years Under the DMCA*, Electronic Frontier Foundation (February 2010) at:

<http://www.eff.org/files/eff-unintended-consequences-12-years.pdf>

## ii **Comments on Provision**

This provision requires countries to structure their TPM laws according to the model adopted in the U.S., which includes a number of specific measures that are not required by the WCT and WPPT.

In particular, it requires countries to create:

- a legal ban on the act of circumventing a technological protection measure that controls access to a protected work (Article 4.9(a)(i));
- a broad legal ban on the manufacture and distribution of certain tools, technologies and devices that can be used to circumvent any TPMs, including access control TPMs and copy control TPMs (Article 4.9(a)(ii) and the definition of "effective technological measure" in Article 4.9(f));
- limited exceptions to these bans for a specified set of 8 purposes mirroring those in the U.S. DMCA (Article 4.9(d) and (e));
- criminal sanctions for violation of the TPM provisions (Article 4.9(a) final sentence and Articles 15.5); and
- specific civil penalties for violation of the TPM provisions, including the ability for judicial authorities to order that a party who loses a civil lawsuit challenging whether there has been a TPM violation be required to pay the court costs and reasonable attorney fees of a prevailing rightsholder (Article 12.2).

Given that the P4 agreement does not include any obligations relating to TPMs and some TPP negotiating countries have not ratified the WCT and WPPT, it is unclear why the TPP agreement should include a specific TPM obligation.

However, if TPP parties decide to include a TPM provision in the TPP agreement, it should be based on the wording of the internationally agreed obligation in Article 11 of the WCT and Article 18 of the WPPT, in order to preserve maximum flexibility for TPP countries to determine how to structure national TPM laws that best meet their domestic priorities, resources, and institutional capacity.



---

iii **Knowledge Requirement**

Actual knowledge of circumvention should be required to impose civil and criminal liability for circumvention of a technological protection measure.

However, paragraph 9(a)(i) does not require that circumvention be done with knowledge. Similar language was used in Article 15.5.7 of CAFTA, Article 15.5.8 of the Morocco FTA and Article 14.5.7 of the Bahrain FTA.

This would impose liability where a person accidentally circumvented or had no subjective knowledge of having circumvented a TPM. For instance, U.S. motion picture copyright owners take the view that playback of a non-region 1 DVD on a multiregion DVD player is a violation of the U.S. DMCA, even where the person who inserts the DVD into a multiregion DVD player has no knowledge of having allegedly circumvented a TPM. An objective knowledge standard would also leave open the possibility that an intermediary, like an ISP or webhosting service, might be held secondarily liable for a user's circumvention offense.

By comparison, Article 17.7.5 of the U.S.-Chile FTA incorporates an actual knowledge standard. It bans the act of knowingly circumventing a technological protection measure, so a person can only be held liable for intentionally circumventing a TPM. More recent FTAs, for instance Article 17.4.7 of the U.S.-Australia FTA and Article 18.4.7(a) of the U.S.-Korea FTA (below), include an actual and constructive (reasonable grounds to know) knowledge standard.

*“knowingly, or having reasonable grounds to know, circumvents without authority any effective technological measure that controls access to a protected work, performance, phonogram, or other subject matter;”*

iv **Ban on Circumvention Devices, Tools and Services**

Like the DMCA, this provision includes a ban on the manufacture, importation, distribution, offering to the public and trafficking in circumvention devices, products and services that meet any of three criteria. Like the DMCA, but in contrast to provisions in other FTAs (e.g., Art. 17.4.7(a)(ii) of the U.S.-Australia FTA), this provision requires accessory liability for those who knowingly market or promote tools for the purpose of circumvention of any effective TPM (i.e. both access control and copy control TPMs).

The drafting history of the WCT indicates that WIPO Member States did not intend to require a ban on tools that can be used to circumvent TPMs. The original document that formed the basis of discussion at the Diplomatic Conference leading up to the adoption of the WCT and WPPT, the Basic Proposal for a Treaty, contained a similar provision prohibiting the manufacture and distribution of circumvention devices, drawn from a U.S. proposal.<sup>iv</sup> However, the majority of WIPO Member States expressly rejected that

---

provision at the Diplomatic Conference, in favor of the more open-ended language in Article 11 of the WCT and Article 18 of the WPPT. (See Article 13(1) of the Basic Proposal for the Substantive Provisions of the Treaty on Certain Questions Concerning the Protection of Literary and Artistic Works, WIPO Document CRNR/DC/4 (Aug. 30, 1996)). The TPP provision would reverse that outcome and remove the flexibility otherwise available to countries in how they may structure legal protection for TPMs under the WIPO Internet Treaties.

The DMCA's provisions governing circumvention tools and services are particularly broad and have had the unintended consequence of restricting or, in some cases, eliminating fair use and other lawful non-infringing uses of technologically protected copyrighted material, and had a substantial detrimental impact on education, user generated content and freedom of expression.

In contrast to the broad prohibition of circumvention tools and services in U.S. law, other countries have implemented more flexible regulations governing access to circumvention tools and services that preserve the ability to obtain access to circumvention tools and services to make lawful non-infringing uses of copyrighted works. For instance, this provision would be inconsistent with sections 226D and 226E of the Copyright Act of 1994 of New Zealand, as amended by the Copyright (New Technologies) Amendment Act 2008 at:

<http://www.legislation.govt.nz/act/public/1994/0143/latest/DLM1705887.html>

See also *EFF Analysis and Implementation Recommendations for the U.S.-Chile FTA TPM Provisions* (2004) on former section 116A(3) of the Copyright Act of 1968 of Australia at:

[http://www.eff.org/files/filenode/FTAA/20040830\\_uschile\\_fta.pdf](http://www.eff.org/files/filenode/FTAA/20040830_uschile_fta.pdf)

#### **<sup>v</sup> Criminal Sanctions**

Like section 1204 of the U.S. law, this provision requires countries to provide criminal procedures and penalties for willful violations of the TPM provisions done for purposes of commercial advantage or financial gain, by anyone other than nonprofit libraries, archives, educational institutions, and public noncommercial broadcasting entities. The WCT and WPPT provisions are silent on this subject. The fear of criminal sanctions in addition to financial liability exacerbates the chilling effect of TPM legislation on socially beneficial, lawful activities.

#### **Other Ways to Structure Penalties in TPM Laws**

The U.S.-Chile FTA contains a number of additional flexibilities for structuring penalties for TPM violations that are less likely to result in harm to other public policy goals.

---

***Limit criminal and monetary liability for scientific research and educational purposes.***

Limiting criminal and monetary liability would mitigate some of the chilling effect of the ban on creating circumvention tools needed for scientific research and provide appropriate incentives for educational purposes.

Article 17.7(5)(b) of the U.S.-Chile FTA, the provision banning the creation or distribution of certain circumvention tools, provides that "due account" must be given to the scientific or educational purpose of conduct in applying criminal measures in implementation legislation. Similar considerations should inform the application of monetary remedies.

***Permit flexibility to exclude civil and criminal liability for innocent infringers.***

Section 1204 of the U.S. Copyright statute excludes criminal liability for non-profit libraries, archives, educational institutions and public broadcasting entities, and section 1203(5)(B) allows a court to remit damages for those entities if they were not aware and had no reason to believe their acts constituted a violation.

Article 17.7.5 of the U.S.-Chile FTA permits an exemption from criminal liability to be granted to nonprofit libraries, archives and educational institutions. It also permits exemption from civil liability, where the circumvention is carried out by those entities in good faith and without knowledge that the conduct is prohibited.

The U.S.- Chile FTA only requires criminal liability for the act of circumvention in "appropriate circumstances," and for violation of the tools ban only where the conduct is willful and for prohibited commercial purposes (Art.17.7.5 (a), (b)). In contrast, section 1201(5)(A) of the U.S. provisions does not remove civil liability for innocent infringers but allows the court to reduce or remit damages where a person was not aware and had no reason to believe that he or she had committed a violation.

<sup>vi</sup> **Scope of Protection**

Most importantly, this provision goes further than the WCT obligation and requires countries to treat violation of the TPM measures as a separate cause of action, independent of any infringement that might occur under the Party's law on copyright and related rights (Art. 4.9(c)). In other words, countries' laws are required to prohibit bypassing rightsholder TPMs even if the circumvention is not tied to any illegal action, for example, where the purpose of the circumvention was to make a non-infringing use of a protected work permitted under a legal exception or limitation, or where there would be no copyright infringement because the content is not copyrightable or in the public domain or because none of the copyright owner's exclusive rights are implicated.

---

The wording of WCT Article 11 clearly contemplates a nexus between legal protection for TPMs and copyright law. It requires WCT Contracting Parties to provide legal protection for TPMs that are used by authors “in connection with the exercise of their rights under this treaty or the Berne Convention” and “that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.”

In the U.S., courts are split as to whether there must be an underlying infringement, and the DMCA, which forms part of the U.S. Copyright Act, does not establish circumvention of TPMs as a separate cause of action. (*See Storage Technology Corporation v. Custom Hardware Engineering*, unreported decision July 2, 2004, 2004 WL 1497688 (D.Mass), vacated on appeal, 421 F.3d 1307 (Fed.Cir. 2005); *The Chamberlain Group, Inc. v. Skylink Technologies, Inc.*, 381 F.3d 1178 (Fed. Cir. 2004); but see *MDY Industries LLC v. Blizzard Entertainment, Inc. et al*, Nos. 09-15932 & 16044 (9th Cir., Dec. 14, 2010)).

Requiring legal protection for TPMs independent of copyright violations is likely to undermine countries’ existing copyright exceptions and limitations and national competition policy. It also runs counter to the emerging consensus from international entities that have investigated the impact of TPM legal regimes, that legal protection against circumvention of TPMs should be tied to the scope of national copyright law.

See Institute for Information Law, University of Amsterdam, *Study on the Implementation and Effect in Member States’ Laws of Directive 2001/29/EC On The Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society* 97, 102–133 (February 2007) available at:

[http://ec.europa.eu/internal\\_market/copyright/docs/studies/infosoc-study\\_en.pdf](http://ec.europa.eu/internal_market/copyright/docs/studies/infosoc-study_en.pdf);  
*Review of Technological Protection Measure Exceptions*, issued by House Standing Committee on Legal and Constitutional Affairs of the House of Representatives, Australian Parliament on March 1, 2006, at:  
<http://www.aph.gov.au/house/committee/laca/protection/report/fullreport.pdf>

This could be addressed by amending Article 4.9(a)(i) to read “knowingly circumvents, for the purpose of infringing a right protected under TPP countries’ national copyright law, without authority any effective technological measure ...”

<sup>vii</sup> **TPM Provisions Should Incorporate a Legislative or Administrative Review and Exemption Process that Permits Exemptions to be Granted for Both the Act of Circumvention and the Tools Necessary to Do So**

Like section 1201(a)(1)(B)-(E) of the U.S. copyright statute, this provision provides for legislative or administrative proceedings that permit three yearly exemptions to the ban on the act of circumvention to make a non-infringing use of a class of copyrighted works. However, like the U.S. law, the provision does not authorize the creation or distribution of the tools that most people will need in order to make use of any exemption granted.

---

Since it is not possible to foresee how the anti-circumvention provisions will impact consumers and important social policies in TPP countries, any provision adopted should incorporate a review of the impact of the circumvention ban, and a process for granting specific exemptions. To create meaningful exemptions for the majority of consumers who do not have the technological expertise to create their own technologies and tools, the legislative or administrative process should permit exemptions to be granted for both the acts and tools necessary to facilitate a permitted circumvention.

In addition, the legislative or administrative process should set a burden of proof for exemption proponents that is reasonable and commensurate with their ability to provide the evidence sought, perhaps employing government ministries to propose exemptions on behalf of affected communities. Once the threshold burden is met, the burden of proof should shift to copyright owners to disprove the need for the exemption sought. While the TPP provision permits the granting of renewable exemptions, it could go further by providing that exemptions previously granted are automatically renewed unless proven to no longer be necessary, and that exemptions granted under the triennial DMCA rulemaking process could automatically be considered adopted in TPP countries.

Six exemptions were granted in 2010 in the most recent U.S. rulemaking for the following classes of works. Several of these exemptions had been granted in previous rulemakings. The U.S. rulemaking does not provide for automatic renewals of exemptions granted in previous rulemakings. These exemptions were regranted after new exemption requests were submitted, on the basis of fresh testimony provided by the applicants that sought them.

(1) Motion pictures on DVDs that are lawfully made and acquired and that are protected by the Content Scrambling System when circumvention is accomplished solely in order to accomplish the incorporation of short portions of motion pictures into new works for the purpose of criticism or comment, and where the person engaging in circumvention believes and has reasonable grounds for believing that circumvention is necessary to fulfill the purpose of the use in the following instances:

- (i) Educational uses by college and university professors and by college and university film and media studies students;
- (ii) Documentary filmmaking;
- (iii) Noncommercial videos.

(2) Computer programs that enable wireless telephone handsets to execute software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications, when they have been lawfully obtained, with computer programs on the telephone handset.

(3) Computer programs, in the form of firmware or software, that enable used wireless telephone handsets to connect to a wireless telecommunications network, when

---

circumvention is initiated by the owner of the copy of the computer program solely in order to connect to a wireless telecommunications network and access to the network is authorized by the operator of the network.

(4) Video games accessible on personal computers and protected by technological protection measures that control access to lawfully obtained works, when circumvention is accomplished solely for the purpose of good faith testing for, investigating, or correcting security flaws or vulnerabilities, if:

- (i) The information derived from the security testing is used primarily to promote the security of the owner or operator of a computer, computer system, or computer network; and
- (ii) The information derived from the security testing is used or maintained in a manner that does not facilitate copyright infringement or a violation of applicable law.

(5) Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete. A dongle shall be considered obsolete if it is no longer manufactured or if a replacement or repair is no longer reasonably available in the commercial marketplace; and

(6) Literary works distributed in ebook format when all existing ebook editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling either of the book's read-aloud function or of screen readers that render the text into a specialized format.

For further information about the administrative proceeding, see:

Librarian of Congress 2010 Determination, July 20, 2010:

<http://www.copyright.gov/fedreg/2010/75fr43825.pdf>

Recommendation of the Copyright Register to the Library of Congress, June 11, 2010:

<http://www.copyright.gov/1201/2010/initialed-registers-recommendation-june-11-2010.pdf>

*DMCA Triennial Rulemaking: Failing the Digital Consumer*, Electronic Frontier Foundation (2005) at:

<[http://w2.eff.org/IP/DMCA/copyrightoffice/DMCA\\_rulemaking\\_broken.pdf](http://w2.eff.org/IP/DMCA/copyrightoffice/DMCA_rulemaking_broken.pdf)>

#### <sup>viii</sup> **Protecting TPMs That Control Access to a Copyrighted Work**

The definition of “effective technological measure” includes both TPMs that control access to a protected work and TPMs that control copying and other uses of protected works. This reflects the U.S. TPM law. However the WCT and WPPT provisions are

---

silent on the question of whether countries are required to protect TPMs that control access to copyrighted works, and legal scholars are divided on this issue.

Since access control TPMs control all access to a copyrighted work, including access for lawful, non copyright-infringing purposes, a legal ban on circumventing access control TPMs would give rightsholders a new right of controlling access to copyrighted works, separate from and potentially unconnected to, the enumerated copyright rights granted to authors under the Berne Convention, the WCT and the WPPT. Thus, a legal prohibition on circumventing access control TPMs could effectively override the traditional boundaries of copyright law.

This could be addressed by amending the scope of the provision as suggested above, or by amending the definition of “effective technological measure” to read “controls access to a protected work, performance, phonogram, or other protected subject matter for the purpose of infringing a right protected under TPP countries’ national copyright law...”.

The definition also raises a second concern. In the U.S. DMCA protection has been claimed for digital content that is not strongly technologically protected in an attempt to prevent reverse-engineering to create interoperable products. For instance, it has been used for content which is not encrypted (and therefore accessible or “in the clear”) and that relies for its security on an interaction between a specific purpose device (such as a console) and a particular cartridge, or a “flag.” To avoid potential impairment of legitimate reverse engineering and the benefits to consumers that flow from more choice of interoperable products, anti-circumvention protection should not be accorded where no attempt has been made to encrypt content – for instance where the only technological measure is a flag or similar measure that can merely be ignored and the content accessed without any form of decryption.

This could be addressed by defining “effective technological measure” to mean encrypted content or content not otherwise accessible to a user without application of information, a process, or treatment that first requires use of a password or other authentication feature, and by expressly excluding information communicated in a natural (non-computer) language.

See *EFF Analysis and Implementation Recommendations for TPM Provisions in U.S.-Chile FTA* at: [http://www.eff.org/files/filenode/FTAA/20040830\\_uschile\\_fta.pdf](http://www.eff.org/files/filenode/FTAA/20040830_uschile_fta.pdf)

#### <sup>ix</sup> **Preventing Anti-competitive Misuse of TPMs**

U.S. copyright owners have used TPMs backed by the DMCA to obtain new monopolies over non-copyrightable products and technologies that interoperate with their copyrighted works. This has had anti-competitive impacts for consumers, and prevented the creation of new interoperable technologies.

---

The DMCA has been used in efforts to lock consumers into purchasing proprietary monopoly-priced products and to prevent the development of legitimate aftermarkets.

For instance, Lexmark, the second largest printer distributor in the U.S., has tried to use the DMCA to block the creation of an aftermarket in recycled printer cartridges that were being sold to consumers at a lower price than Lexmark's own authorized refilled cartridges (Lexmark International, Inc. v. Static Control Components, Inc., 253 F.Supp.2d 943 (E.D. Ky. 2003), *vacated and remanded on other grounds*, 387 F.3d 522 (6th Cir. 2004)). A garage door manufacturer, Chamberlain Group, tried to use the DMCA to ban the sale of its competitor's universal garage remote control opener (The Chamberlain Group, Inc. v. Skylink Technologies, Inc., (N.D. Ill., unreported Civil Action No. 02 C 6376); *aff'd on appeal*, 381 F.3d 1178 (Fed. Cir. 2004)). A telecommunications company has used the DMCA to block cell phone unlocking services, and a proprietary data storage company used the DMCA to ban its customers' use of an independent computer maintenance service (Storage Technology Corporation v. Custom Hardware Engineering, unreported decision July 2, 2004, 2004 WL 1497688 (D.Mass.), *vacated on appeal*, 421 F.3d 1307 (Fed.Cir. 2005); TracFone Wireless, Inc.v. SOL Wireless Group, Inc., No. 05-23279-CIV-Altonaga/Turnoff (S.D. Fla, Feb. 28, 2006).

While the "no mandate" clause in Article 4.9(b) is helpful, potential misuse could also be minimized by excluding certain measures from the definition of technological protection measure, as has been done in section 10 of the Australian Copyright Act of 1968, as amended in 2007. See:

[http://www.austlii.edu.au/au/legis/cth/consol\\_act/ca1968133/s10.html#access\\_control\\_technological\\_protection\\_measure](http://www.austlii.edu.au/au/legis/cth/consol_act/ca1968133/s10.html#access_control_technological_protection_measure)

It excludes region coding TPMs on movies and computer programs (including video games) and computer programs that are embedded in devices that restrict the use of goods (other than the work) or services. This would appear to minimize the likelihood of the misuse described above.

Section 10 of the Australian Copyright Act defines "technological protection measure" to mean:

*" (a) an access control technological protection measure; or  
(b) a device, product, technology or component (including a computer program) that:*

*(i) is used in Australia or a qualifying country 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*

*(ii) in the normal course of its operation, prevents, inhibits or restricts the doing of an act comprised in the copyright;*

*but does not include such a device, product, technology or component to the extent that it:*



---

(iii) if the work or other subject-matter is a cinematograph film or computer program (including a computer game)--controls geographic market segmentation by preventing the playback in Australia of a non-infringing copy of the work or other subject-matter acquired outside Australia; or

(iv) if the work is a computer program that is embodied in a machine or device--restricts the use of goods (other than the work) or services in relation to the machine or device.”

And “access control technological protection measure” to mean:

“a device, product, technology or component (including a computer program) that:

(a) is used in Australia or a qualifying country:

(i) 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

(ii) in connection with the exercise of the copyright; and

(b) in the normal course of its operation, controls access to the work or other subject-matter;

but does not include such a device, product, technology or component to the extent that it:

(c) if the work or other subject-matter is a cinematograph film or computer program (including a computer game)--controls geographic market segmentation by preventing the playback in Australia of a non-infringing copy of the work or other subject-matter acquired outside Australia; or

(d) if the work is a computer program that is embodied in a machine or device--restricts the use of goods (other than the work) or services in relation to the machine or device.”

Finally, the Australian law also contains an important remedy to combat possible misuses of TPMs for non-copyright infringing purposes such as attempted control of interoperable technologies. It allows a person who has been threatened with a groundless threat of TPM legal proceedings to bring legal action for an order declaring that the threat is unjustifiable, an injunction to restrain the copyright owner or exclusive licensee from continuing with the groundless threat, or an award of damages for loss suffered as a result of the threat.

See section 202A of Australian Copyright Act at:

[http://www.austlii.edu.au/au/legis/cth/consol\\_act/ca1968133/s202a.html](http://www.austlii.edu.au/au/legis/cth/consol_act/ca1968133/s202a.html)

**“Groundless threats of legal proceedings in relation to technological protection measures**

- 
- (1) If a person (the first person ) threatens another person with an action under Subdivision A of Division 2A of Part V, a person aggrieved may bring an action against the first person.

*Note:* Subdivision A of Division 2A of Part V establishes causes of action that relate to circumventing an access control technological protection measure (section 116AN), manufacturing etc. a circumvention device for a technological protection measure (section 116AO) and providing etc. a circumvention service for a technological protection measure (section 116AP).

- (2) An action may be brought under this section whether or not the first person is the owner or exclusive licensee of the copyright in the work or other subject-matter to which the threatened action relates.
- (3) The mere notification that a work or other subject-matter is protected by a technological protection measure does not constitute a threat of an action within the meaning of this section.
- (4) In an action under this section, the orders a court may make include the following:
- (a) an order declaring that the threat is unjustifiable;
  - (b) an order granting an injunction restraining the first person from continuing to make the threat;
  - (c) an order awarding such damages (if any) for loss that the person aggrieved has suffered as a result of the making of the threat.
- (5) The court must not make an order under subsection (4) if the first person satisfies the court that an action under Subdivision A of Division 2A of Part V has reasonable prospects of success.
- (6) Nothing in this section renders a barrister or solicitor of the High Court, or of the Supreme Court of a State or Territory, liable to an action under this section in respect of an act done in his or her professional capacity on behalf of a client.
- (7) If an action under this section is brought:
- (a) the first person may apply, by way of counterclaim, for relief to which he or she would be entitled in an action under Subdivision A of Division 2A of Part V; and
  - (b) the provisions of Part V apply as if the counterclaim were an action brought by the first person under that Subdivision.”

---

<sup>x</sup> **Statutory Damages**

The TPP provisions require countries to adopt a statutory damages regime for TPM violations. Section 1203(3) of the U.S. copyright statute sets out the statutory damages requirements for violations of the U.S. TPM provisions.

The U.S. copyright regime for pre-established or statutory damages for copyright infringement is highly controversial within the U.S. This is particularly true for statutory damages for TPM violations. As many TPP negotiating countries do not have statutory damages regimes, it is inappropriate to include an obligation for countries to adopt a statutory damages regime either for copyright infringement or for TPM violations.

The possibility of being subject to often disproportionately high statutory damages impedes computer security research and innovation because computer security researchers and innovators will be reluctant to undertake research or create new technologies and software that interoperates with TPM protected copyrighted works if they may face crippling damages claims for doing so.

In recognition of this, section 1203(5) of the U.S. copyright statute gives courts the discretion to reduce or remit damages awards where the court finds that the person was not aware and had no reason to believe that its acts violated the TPM provisions. Section 1203(5)(B) also requires courts to do so for non-profit libraries, archives, educational institutions and public broadcasting entities in the same circumstances.

The TPP provisions do not include a similar limitation. If the TPP includes a requirement for countries to adopt statutory damages for TPM violations, it should permit judicial authorities to reduce or remit statutory damages for innocent violations to reduce the chilling effect of statutory damages claims on scientific and computer security research, individuals' freedom to tinker, and technological innovation.

<sup>xi</sup> **Awards of Court Costs and Attorney Fees In TPM Lawsuits**

Article 12.12 (c) requires countries to give judicial authorities the power to order that a person who is unsuccessful in defending a TPM lawsuit must pay the court fees and costs and reasonable attorney's fees of the prevailing right holder who has brought the lawsuit against him or her.

By comparison, section 1203(b)(4) and (5) of the U.S. Copyright statute gives courts the discretion to make such orders. Article 12.12(c) could be read as going beyond U.S. law because it does not specify that judicial authorities should have discretion to make such awards. What is now the exception could accordingly become the rule in the U.S. and in all other TPP countries.

---

As the numerous threats and cases under the U.S. DMCA provisions have demonstrated, it is often not easy to determine whether a particular act of computer security research or other activity is lawful or would be a violation of the U.S. TPM provisions. (See for instance, Sony's threats to Aibo electronic toy dog hobbyists who modified their dogs to "dance" in EFF Unintended Consequences report at <http://www.eff.org/wp/unintended-consequences-under-dmca>). In this context, adding an additional penalty to the fines already imposed for violation of the TPM provisions on those who unsuccessfully defend TPM lawsuits will further chill individuals' freedom to tinker with technologies that they have purchased, impede non-copyright infringing reverse engineering and the development of free and open source software, and stifle technological innovation.