For the attention of:

Committee Secretary
House of Representatives Standing Committee on Legal and Constitutional Affairs laca.reps@aph.gov.au

Please find following Cybersource's followup to our submission in respect of the Inquiry Into Technological Protection Measures (TPM) Exceptions.

By: Steven D'Aprano, Operations Manager
On behalf of: Cybersource Pty Ltd (Cybersource)

Followup to Questions on Notice by Ms Roxon and Mr Melham.
==========

(1) Mr Melham asked what was the status quo relating to reverse engineering software before the introduction of the US-Australia FTA.

According to Section 47F of the Copyright Act 1968, the copyright in a computer is not infringed by the making of a reproduction or adaptation of the work for the purposes of:

(b)(i) testing in good faith the security of the original copy, or of a computer system or network of which the original copy is a part;

(ii) investigating, or correcting, in good faith a security flaw in, or the vulnerability to unauthorised access of, the original copy, or of a computer system or network of which the original copy is a part;

Likewise, Section 47E allows an exemption for the purposes of correcting errors, and Section 47D allows an exemption for the purposes of making interoperable products.

It is our understanding that the prohibition against circumventing TPMs can and will render the above copyright exemptions meaningless. While the Copyright Act allows licensees of computer software to fix security flaws in software, if those security flaws are behind a TPM, it will become a criminal offense to do so.

This is no hypothetical issue. As the Sony-BMG case demonstrates, there can be wide-ranging and severe security holes inadvertently hidden behind TPMs. For example:

* The Sony spy software protected by a TPM can be installed on users' computers even if the user clicks "Decline" to the license agreement: http://www.freedom-to-tinker.com/?p=936

* More than half a million networks were infected by the Sony rootkit, including military networks: http://www.wired.com/news/privacy/0,1848,69573,00.html

* The security patch released by Sony to repair the damage caused by their TPM itself contained an even more dangerous security hole: http://blogs.washingtonpost.com/securityfix/2005/11/sony_uninstall_.html

Less reputable companies have already used copyright law to try to intimidate computer security companies. One example is here:

http://www.theregister.co.uk/2005/11/14/spymon/

The TPM legislation will be a boon to less reputable companies, allowing them to threaten computer security professionals with jail for bypassing their spyware or keyloggers. Whether the Courts would actually side with the spyware companies or not is irrelevant: few security professionals would be willing to take the risk of a jail term for investigating harmful spyware protected by a TPM.

The mere threat of prosecution for bypassing a TPM will have a chilling effect on computer professionals, who will be unwilling to investigate further examples of software with security holes which are protected by TPMs.

As the Assistant Secretary of the US Department of Homeland Security made clear recently, this could have a profound and harmful effect on the security of the nation's critical IT infrastructure. (See the Washington Post article given as evidence at the Public Hearing on Tuesday 15th November for further details.)

It is Cybersource's position that the Government should create an exemption to the TPM legislation which allows the status quo as per the Copyright Act 1968, Sections 47D, 47E and 47F. This would explicitly protect good faith investigation and correction of security flaws and errors, as well as interoperability.

(2) Cybersource has expressed serious concern that the TPM legislation will have the inadvertent side-effect of protecting companies who themselves infringe copyright, hiding such stolen code behind a TPM in order to avoid detection. Again, the Sony-BMG case is a good example: the code of their TPM has been reverse-engineered and Open Source software has apparently been discovered in Sony's software. Sony's stated intention was to protect their own copyrighted material, but on the evidence so far, they have done so by illegally using Open Source software.

See for example:

http://sam.zoy.org/blog/2005-11-21-suspicious-activity-indeed
http://www.freedom-to-tinker.com/?p=940

The copyright holder of the software found hidden behind the TPM, Mr Hocevar, is apparently living in France. If he lived in Australia, it is questionable that he would take the risk of prosecution. It is likely that there are many more examples of infringing companies hiding behind TPM to avoid detection.

Like all programmers, Open Source programmers have the protection of Copyright law, but that protection is only as strong as their ability to detect infringement. By hiding behind a TPM, infringers can steal copyrighted software with impunity. We ask for the current limited copyright exemptions to be made exemptions to the TPM legislation.

(3) Both Mr Melham and Ms Roxon were concerned that Cybersource was looking to have an open-ended exemption allowing us to go on fishing expeditions looking for infringing software hidden behind TPMs.

We would like to assure the Committee that our request is much more limited than that.

The Copyright Act 1968 gives limited exemptions: for example, Section 47D allows an exemption for the purposes of interoperability, Section 47E for the purposes of correcting errors, and Section 47F for the purposes of security testing. We ask that these limited and reasonable exemptions to Copyright law be extended to the TPM legislation.

It is Cybersource's position that to have the TPM legislation take away rights already granted will be harmful to not only the Australian Open Source industry but also the security and safety of Australian IT systems in general.

We are looking for one new exemption: the right to bypass TPMs for the purposes of enforcing our own copyright. This was never needed before, because it was not needed until now.

We do not expect an exemption to be granted for any use from an infringing copy of a computer program: any exemptions should only apply to legally licensed copies.

Secondly, as per the Copyright Act Section 47F, we ask only for an exemption for good faith investigations. What we are asking for is no more open-ended than existing copyright exemptions.

Cybersource would like to thank you for this opportunity.

Yours sincerely,

Steven D'Aprano
on behalf of Cybersource Pty Ltd.