Tremble, Kate (REPS)

From: Steven D'Aprano [steve@cybersource.com.au]
Sent: Friday, 7 October 2005 6:04 PM
To: Committee, LACA (REPS)
Subject: Submission into Inquiry Into TPM

For the attention of:

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

Please find following a 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)

Summary:
========

Cybersource is very concerned that the provisions relating to Technological Protection Measures (TPM) can and will be used as anti-competitive and discriminatory measures that will disadvantage companies such as ourselves. In particular, we are very concerned that legislation enforcing TPMs will have the paradoxical effect of hiding and protecting certain types of copyright infringment, putting companies such as ourselves at a serious competitive disadvantage.

We believe that explicit exemptions allowing circumvention for the purposes of investigating copyright infringement and for the purposes of interoperability are needed.

Discussion:
==========

Cybersource is an IT consultancy specialising in Open Source software, including software development. As such, we are both creators and users of copyrighted software.

Specifically, the Open Source software model relies strongly on copyright to enforce our rights. Unlike closed-source and proprietary software suppliers, the Open Source model makes the human-readable source code readily available. We believe that this model has many competitive advantages over the closed-source model, for both users and creators. We work hard at coming up with innovative solutions to computer problems, and it is our belief that Open Source is a better, more efficient way of software development and distribution than the closed-source model which attempts to keep the human-readable source code secret.

Nor are we alone: we are a member of the Open Source Industry Australia Limited (OSIA) industry group, whose membership includes 250 businesses, organisations and consultants. Likewise, industry leaders like IBM, Red Hat, and Sun have also moved partly or wholly towards an Open Source business model.

We believe that Open Source is the way of the future for the IT industry. Time and hard work will see if we are right: we are prepared to live or die by our ability to compete in the marketplace. However, the TPM provisions impose a serious competitive disadvantage on Open Source companies such as ourselves.

One of the principles of Open Source is to "share and share alike": if we distribute Open Source software to somebody, they are permitted by the licence to make derivative works provided that they return those improvements back to us. This works well: the Internet is built on such

Open Source technologies, the Linux operating system is based on such a process, and such global giants as IBM and Novell are committed to it.

Open Source software is not in the public domain. It is supplied under a legal licence, just as closed source software from Microsoft or Apple is supplied under a licence. Open Source relies on strong copyright law to enforce the licence, just as any other software supplier does.

Because we distribute the source code to our programs, not just unreadable machine code, people can insert our copyrighted work into their own source code, making a derivative work, and compile that derivative work into a machine-readable form. So long as they abide by the Open Source licence and return improvements and changes they make to us, this is a legal use of our works, and we are satisfied.

But, either maliciously or through ignorance, some people wrongly believe that they can break the terms of the licence. They reason that since they only distribute the machine code, which is not readable by humans, they can plagiarise or otherwise misappropriate our copyrighted works with impunity. That gives them the benefit of our labour without either compensating us, or abiding by the not unreasonable provisions of our licence.

Fortunately they are wrong. There are techniques that a skilled practitioner can use to detect such copyright violations even in unreadable machine code. See, for example, this alleged infringement by the developers of CherryOS:

http://www.ht-technology.com/cherryos-pearpc/cherryos-pearpc.html

This website tracks violations of one specific Open Source licence:

http://gpl-violations.org/

This gives a partial list of 18 proven or alleged licence infringements of this one licence this year. A particularly worrying case involves Fortinet, who allegedly attempted to use a TPM to encrypt their product in such a way as to hide the fact of their violation:

http://gpl-violations.org/news/20050414-fortinet-injunction.html

Had this case occurred in Australia instead of Germany, the infringing party could hide behind the TPM provisions of the Act. Open Source developers such as ourselves could not legally circumvent their protection measures in order to gather evidence that they have infringed our copyright, and without that evidence, it would be difficult or impossible to take legal action against them.

This ability for copyright infringers to hide behind the anti-circumvention law is surely an unexpected and unwanted side-effect of the law. We do not believe that the government intended to give copyright thieves and cheats a Get Out Of Jail Free card to steal from Open Source developers such as ourselves.

We believe that the government should create an explicit exemption to the TPM legislation to allow copyright holders to circumvent TPMs for the purposes of investigating copyright infringement. This exemption will, of course, benefit all copyright holders, not just Open Source developers, but it is especially needed for Open Source developers as we are particularly at risk of copyright infringement.

The ability of copyright infringers to hide behind the TPM legislation is just one of the anti-competitive and discriminatory side-effects of the Act. A particularly egregious problem involves the use of TPMs to lock consumers into a specific product by effectively holding the consumer's data hostage.

Software is usually only useful with data. For instance, consumers create data (letters, documents, novels, etc.) using a word processor program, or numeric data using a spreadsheet program. The user's data is stored in a file format particular to the program used to create that data.

Although copyright in the program is held by the software developer, the copyright in the data is held by the software user. However, the risk is that the software developer may choose to keep their file format secret. This means that once the user's data is stored in that file format, the consumer cannot get access to their own intellectual property except through that particular software. If it means losing all their existing data, or re-keying it manually from print-outs, few users will change the software they use.

(A counter-example is Internet standards, such as the file format used for web pages. Because the HTML file format is a vendor-neutral standard, there is no lock-in, and web developers are free to use any number of web page editors, safe in the knowledge that no program can lock up their intellectual property in a secret format.)

Historically, Australian law has recognised this anti-competitive behaviour, and the risks it poses, and have explicitly allowed the right to reverse-engineer software for the purpose of interoperability.

Unfortunately, it is a trivial matter to wrap a file format up in a TPM layer in such a way that any attempt to reverse-engineer the format would require circumventing that TPM layer. This would allow vendors to effectively hold consumers' intellectual property hostage: if you use a competing product, you will effectively lose your existing data.

I do not believe that the intention of the government is to allow, let alone encourage, this sort of anti-social, anti-competitive behaviour. In effect, it would allow the software developer to limit or even prohibit software users' accessing their own intellectual property. Imagine a business with their critical financial data locked up in a proprietary database. It is no stretch of the imagination to see the database vendor charging an every-increasing yearly subscription fee. With their data locked in, the business is unable to escape except at the cost of losing access to their data. Data which I must emphasis they, and not the database vendor, own.

An exemption to the anti-circumvention law is absolutely critical to prevent software providers, particularly monopolists or near monopolists, from limiting users' right to access their own intellectual property or breaking interoperability. To protect these essential rights, there must be a TPM exemption for the purposes of allowing interoperability.

I thank you for this opportunity to make a submission.

Yours sincerely,

Steven D'Aprano
Operations Manager
on behalf of Cybersource Pty Ltd.

--
Steven D'Aprano
Operations Manager
Cybersource Pty Ltd, ABN 13 053 904 082
Level 4, 10-16 Queen St, Melbourne VIC 3000
Tel: +61 3 9621 2377 Fax: +61 3 9621 2477
Web: http://www.cybersource.com.au