Janet Hawtin Clarence Gardens South Australia 5039
lucychili@gmail.com

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

Re Submission to review Technological Protection Measures Exceptions.

I am writing regarding the DMCA TPM exemptions, as a citizen concerned for the rights available to our younger generations. I would like to offer the following suggestions regarding the application of TPMs and the DMCA..

I am responding generally but do believe that my comments will be relevant to the activities of libraries, archives and other cultural institutions, the activities of educational and research institutions, the use of databases by researchers, activities conducted by, or on behalf of, people with disabilities, the activities of open source software developers, and activities conducted in relation to regional coding of digital technologies.

I am proposing guidelines or conditions under which the TPM and CDMA should operate.
These should make it possible for people using digital media (including those listed above)

- to know in advance if the product is protected and
- to know what their usual rights are with regard to digital media and
- how those differ with a product which is covered by a TPM.

This approach seems to me the most practical way of ensuring that legitimate uses of media can be undertaken with confidence, and copyright of media can be appropriately protected.

Long fuse on impact and feedback

Firstly I am concerned that there will be people impacted by this law who do not realise this yet. This means that the feedback being received currently will be forwarded by those who stand to benefit from the law and by those few who recognise the direct risks of the DMCA on their rights.

Many of the industries involved in interacting with digital media would not consider themselves involved in computing as such. Chips are used in automotive, scientific and medical equipment, agriculture, mobile phones, white-goods, shop tills, merchant card access and atms, the scope is broad. Computer chips and digital logic are the pervasive technology of our time. The potential impact then of this law is likely to unfold as different business sectors and community groups find it applies to them.

DMCA Scope

I believe that the best way to incorporate the DMCA is to get to the core of its original intent and to restrict its effect to those situations of copyright breach which are not a natural and healthy part of a vibrant and confident culture and industry, and to balance the impact of this kind of restriction with long overdue definition and education of digital access rights for people within Australia as well as real tangible support for open standards and community owned resources.

The DMCA law should not operate as the default state of play for digital rights. It should be a lock down of a pre-approved and specific component of software or hardware in order to protect copyright.

Digital infrastructure and open standards

We live in a time where the technological infrastructure around us is more 'core' to our daily functioning as a nation than our roads. As a result of awareness that this infrastructure is universally important to culture and trade many people, organisations businesses and countries have gone to a lot of effort to commit to open standards to facilitate transparency in the technologies which are important to all people using digital modes of communication.

Consistent with these commitments and values I feel it is important for Australian legislators to provide a transparent and predictable legal framework of access rights so that people can learn, explore, do business, invent, develop secondary brands to interact with other brands of software etc. Basically to life a full cultural and business life.

Within an environment such as this business people and developers could make decisions regarding investment and invention without concern that their work could become illegal if a primary publisher or manufacturer introduces a TPM to shut their product or process out of a market. The DMCA could still have its intended purpose in this environment.

Rights come with responsibilities

I feel that the DMCA provides publishers and manufacturers with rights which should be balanced with responsibilities. Having a locked down black box of software on one's computer is a considerable trust to place in the publisher of the software. This should bring with it relevant responsibilities and conditions. A product should only be covered by the

TPM and DMCA laws only if it is appropriate.
Some examples of useful conditions:

- Prior to lock down being permitted the publisher/manufacturer would need to prove that the software has contains only software which the DMCA copyright applicant has proven to be wholly their own property.
  In situations where a third party is contesting the copyright of the product there should be an opportunity to unpack the software legally in order to confirm or deny these concerns. In situations where a developer suspects a product of breaking their own copyright it would be reasonable to expect that they should be able to look at the material before venturing into court.

- The product and its TPM can guarantee that such a lock down has no impact on the function of other software on a system. It is not appropriate for a TPM to apply where its operation will break or impact on other applications and where it would be reasonable for the user to turn off a TPM in order to regain function of other applications. A product may have an active TPM which is not then defensible if for example it disables cookies or impacts on java thereby impacting on other applications.
  Inter-product technologies inherently need to be transparent so that they can be understood by developers of interacting products. DMCA and TPM should not be applicable for these kinds of technologies. I believe this has been considered for networking technologies but I feel that it should be expressed more broadly to include intra-computer interactions between applications as well.
  Technologies which provide interfacing between different systems and enable a diverse network of technologies to interact should be legally able to do so. Open standards are an important move forwards which our generation has made. Open formats have taken a lot of work by many groups to keep information and resources from being locked into post-sale license-defined dead-ends. Develop clear guidelines for when open standards need to have right of way or better still - when it is safe for a product to be locked down because is is sufficiently self contained.

- The DMCA and TPM laws should specifically not be used to exclude other software from the market.
  The impact of the DMCA on Australian industry is potentially broad because the law potentially lays the foundation for a primary brand to control the right to develop and deploy software which interacts with their brand. Australia being one of the smaller development and manufacturing industries would have a high proportion of 'secondary' brands -ie products which would depend on their interaction with other primary brand software in order to function. Secondary brand software developed overseas for use in local product development could also be impacted because it is in use and deployment as well as development that a primary brand could deem a secondary or supporting brand is non-compliant. This should not be an appropriate use for the DMCA as it would provide a framework for a few brands to monopolise the digital marketplace by restricting developers and limiting choices for users.

- A product which collects personal information of the user should not be protected by a TPM.
  I feel it is inappropriate for a package which collects information about me as person or as a web user to be collected in locked down software which may not be scrutinised for appropriate storage and use of that data.

- A product which is involuntarily installed such as adware, spyware or any program which is installed without prior acceptance by the user of the specifics of the TPM and associated legality should not be protected.
  Information required by a consumer/developer in order to make an informed purchase:

  - Full description of the tpm (ie what must not be touched)
  - Full explanation of how the software may be legally used
  - Full description of how the software may not be legally used

- Defensive unpacking should be legal.
  As marketing becomes more pervasive and intrusive software developers are making tools which help people to defend their computers from unwanted marketing or intrusion. One persons great product or interactive advertising thing can be another persons unwanted spam spyware or virus.
  Developers who unpack these things and write vaccines or detectors are the white blood cell count of the Internet. Criminalising this kind of activity is not going to make the Internet a more law abiding place.
  Even making people reluctant to unpack a virus in case it will be an illegal act will slow down responses by skilled individuals to damaging virii. The distributed flexible quick response to these threats is important for a healthy Internet. Careful appreciation of when a person could consider a product undesirable/illegal and could reasonably be aiming to unpack it to defend against it will need be considered when applying this law. Preferably this could be seen as a kind of unpacking which does not infringe copyright and therefore is legal anyway.

- Where the product malfunctions the user or their agent should be able to investigate legally.
  Where a person is repairing or bypassing a broken TPM protected product in order to repair a system.
  This should not be illegal especially in cases where there is health risk or other associated loss or damage as a

result of the malfunction. (eg bypass of electronic ignition on a car where the driver is in a remote situation)

- Custom hardware interfaces should be used if a product should not legally plug into standard hardware. This should be made clear to a consumer prior to purchase. If a new software or hardware "thing" could be physically plugged into an open standard hardware socket but should not legally do so then it would be appropriate to require that the hardware did not fit 'illegal' standard sockets but had a custom hardware interface which made it easier for post-purchase users(eg tech support staff in a university) to see that a specific product had restricted legal application.

I believe that these responsibilities make it possible for Australian users and developers to make informed decisions about their interaction with TPM software and for users to retain rights to manage their own computers. It is important to retain transparency where that is appropriate and to minimise barriers to innovation and market entry for smaller companies and unfunded researchers.

Without these responsibilities it would be very difficult for a person to determine if they were breaking the law because the rights and limits will vary according to the product in question. I feel this is very important. How does a smaller or even large developer of a physical product or intellectual property know IF they are in violation and of how many "patents"/"propriety interfaces" they are in violation of. Clearly this needs to be information which is readily available for consumers and developers prior to purchase or interaction with the software.

Digital access rights

The other facet of this issue is that this law is being introduced into a country which needs to update the fundamental digital access rights for users and developers and to provide a comprehensive education program to enable Australians to understand their rights and to make the most of them.

These updated digital access rights should include:

- Right to ones own content or voice or expression distinct from any rights of a medium which is used to express it.(eg. If I take a photo the photo should be mine not the property of the person who developed the camera or the photo unless explicitly negotiated with the originator of the item.)
  The original carrier model should be applicable for digital media too.
  A telecommunications group may own the mode of communication but my conversation should be mine.
  This should be consistent in a digital environment (eg. with email, mailing lists, blogs etc.)

- Right to interact with media, to quote it, comment on it, print it out, discuss it with friends, learn about how it is made, learn about how other similar things might be made. These rights should be the default expectation. DMCA with TPM should be a specific exception applied in situations where the publisher has demonstrated that their product is appropriate to cover with this legal lock down.

Goals for digital access rights management laws

Australia is promoted as a thinking nation. This scholarship and innovative culture is dependent on our ability to access a wealth of resources with which we can fully interact.
Australia is a nation with a rural population disadvantaged by lack of ready access to physical resources.
Digital media are an important resource for rural communities. In a nation where people are increasingly relying on access to digital books and resources it is important to support authors manufacturers and publishers who operate in a way which facilitates the continued rights of other Australians. Australian government should support use of open formats so that more media is available which is truly accessible.

We should all have a fundamental right to access our heritage. To entertain, explore and inform each other is a cornerstone value of all democracies. For those publishers looking to lock down their products we should be aiming to provide them with a better understanding of why these rights are important and how authors and developers can generate income while ensuring the community has the best possible chance of benefiting from their work.

Restrictions on some ebooks include that they should not be read aloud, no text should be copied from them, they may not be printed, shared, lent or given away. This represents a very real reduction in the functionality of a book if this becomes the default format and legal constraint on future books. Active support of publishing models and education programs which enable authors, publishers and manufacturers to make their works accessible and open are going to be an important counterpoint to restrictive copyright laws and to ensure that a digital book of the future is at least as useful as the paper book of the past.

We have well developed and stable models in place for authorship copyright and publishing/production rights.
In place now. They have worked well for at least a hundred years and have survived the introduction of steam, electricity and the Internet. They work now.

In conclusion I am suggesting that the DMCA law be defined in such a way that it is possible for users and developers to avoid isolationist software, or to choose to purchase and use it with knowledge of its legal constraints.
Digital technologies are inherently about interconnectivity. Transparency is often important.
Lock down software should be the exception and not the rule.

Australia is a nation. That means we have cultural and business interests of our own. We are not defining and defending what is important to our cultural heritage and business and scientific development.
We cannot expect our competitors (even friendly ones) to create law with our interests at heart it is not their job...
I would like to see Australian politicians/legislators put real thought, heart and commitment back into defining what this country can be. More than a minor flock of bonded consumers I hope.

To put my self where my mouth is: If there are improvements made to secure the digital access rights of Australians I would be interested in participating in education programs to help people understand their rights and responsibilities.
I currently undertake computing work in the community and would be happy to include information on these topics as part of this work.

Regards

Janet Hawtin