

Submission

ACTA - Enforcement in the Digital
Environment

Tech Liberty

<http://techliberty.org.nz>

PO Box 5641
Lambton Quay
Wellington

Introduction

Thank you for the opportunity to make a submission on the provisions for Enforcement in the Digital Environment for the ACTA treaty negotiations.

About this Submission

We have decided to only respond to the questions posed in your request for submissions. This should not be taken to signify our approval of the overall ACTA process, the goals of ACTA, or New Zealand's participation in it.

About the Submitter

Tech Liberty is dedicated to protecting people's rights in the areas of the Internet and technology. We make submissions on public policy, help to educate people about their rights, and defend those whose rights are being infringed.

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Liability of Third Parties for Infringement

Safe Harbours for ISPs and Specifying When an ISP is Liable

Should ACTA include provisions requiring ACTA parties to provide safe harbours for ISPs for certain infringing activities? If so, what infringing activities should be covered by the safe harbours?

Should ISPs be additionally required to meet any conditions in order to qualify for the safe harbours? If so, what should those conditions be?

Would this alternative approach better achieve the objective of giving greater legal certainty to ISPs, whilst also ensuring that measures are available to right holders to take adequate and effective action against infringement?

Should ACTA parties be given the discretion to choose between implementing one or the other of these two approaches to achieve this objective?

Our Response

ISP's Role

It is our understanding that an ISP can have the following relationships to data passing through their network:

- a) They can be acting as a data conduit between one of their users and the rest of the Internet.
- b) They can be providing a hosting platform that their clients publish material on (i.e. the ISP has a webserver with multiple clients that publish material on it).
- c) The ISP can be publishing material itself (e.g. the ISP's own website).

In case a), **data conduit**, we do not accept that the ISP is or can be liable for the actions of their account holders. Firstly, ISPs often cannot tell what their users are doing on the Internet. Secondly, the ISP is merely acting as a data service and it would be unreasonable and contrary to the principles of natural justice to blame them for the actions of others.

In case b), **hosting**, the ISP is again not responsible for the actions of others. As the content is directly provided by others with no inspection or approval by the ISP, there is no question of the ISP being liable for it. The ISP is able to take the site offline but such a major step should only be done at the order of the court.

In case c), **publishing**, the ISP is clearly responsible for the material that they publish. The ISP will be the target of legal action if they break the law.

Safe Harbour

We note that New Zealand does offer a "safe harbour" provision where, if an ISP's server hosts material, someone can claim that it infringes their rights and the ISP can protect itself by taking the material down (this corresponds to case (b) in our list above).

We believe that this law is in error and is offensive to people's rights. It gives too much unchecked power to complainants and can be used to undermine free speech (e.g. if you publish contentious material, someone can submit a baseless claim to get it taken down, safe in the knowledge that by the time it's reinstated the material will be out of date).

A much better solution is that in the proposed section 92A of the NZ Copyright Act where, acknowledging that ISPs are in the unique position of being able to identify the account holder for a particular IP address at a particular time, they have a responsibility to pass on notices from complainants. This allows for complainants to protect their interests while also protecting the privacy rights of the user, at only a small (recoverable) cost to the ISP.

Recommendations

1. The ACTA treaty should note that ISPs are not liable for the actions of their users.
2. That ACTA includes a "notice and counter-notice" regime where complainants can pay ISPs to deliver a notice to the account holder for an IP address at a particular time, and the ISP can pass responses back to the complainant.

Other Matters

Identifying Infringing Users

Under what circumstances should right holders be able to expeditiously obtain information an ISP about the identity of the relevant user who is engaging in the infringing activity?

Our Response

While we have argued that ISPs are not liable for the actions of their users, we do acknowledge that ISPs are in a unique position as the only people able to identify which of their account holders is using a particular IP address at a particular time. Without this information, complainants are severely hindered in their ability to pursue people who they believe are infringing their rights.

However, we also believe that the ISP's account holders have a right to privacy. Their identity should not be given out lightly, especially not in response to unproven accusations.

In accordance with established NZ law, we believe that the courts are the appropriate place for these conflicting interests to be weighed against each other. Complainants should only be able to obtain identities from ISPs after showing due cause to a court and receiving an appropriate order.

Recommendations

3. That ACTA specifies that complainants should be able to obtain the identity of a user from the ISP only after a court order has been obtained.

Promoting Cooperation Between ISPs and Rights Holders

Should parties to ACTA be required to promote domestically the development of mutually supportive relationships between ISPs and right holders to deal effectively with infringements of intellectual property rights taking place via the Internet? If so, how might a party promote such a relationship?

Our Response

As ISPs and rights holders have no common interests there seems little point in trying to encourage them into mutually supportive relationships, apart from what they choose themselves.

Recommendations

4. That ACTA makes no attempt to encourage mutually supportive relationships between ISPs and rights holders.

Technological Protection Measures

What enforcement measures should ACTA contain for remedying and deterring the circumvention of a TPM used to control access to, or prevent unauthorised copying, playing or distribution of, a copyright work?

Our Response

About TPMs

We do not object to people using technological protection measures in their products. However, we note that these technological measures often go far beyond reasonable protection and prevent purchasers from using their products as they are entitled to. Some examples:

Example 1 - a purchased ebook would not let users copy and paste text for the purposes of quotation, nor would it allow even a single page to be printed.

Example 2 - music CDs have included TPM that have prevented them being played in computers or other classes of device.

Example 3 – movie DVDs include region codes that stop a person legally buying a DVD in one country, moving to another country and playing it in a DVD player purchased in the second country.

In all three cases the purchaser had to circumvent the TPMs to let the purchaser enjoy the rights that they had paid money for.

TPMs and Current New Zealand Law

New Zealand Copyright law recognises that there is a public interest in setting restrictions on the conditions that copyright holders can impose on their licenses. For example, it gives people the right to make backups, convert works into Braille, and quote excerpts for review, regardless of the views of the copyright holder.

The law also recognises that there valid reasons for circumventing TPMs and contains provisions allowing that. However, it is confused in that it tries to limit the ability to circumvent TPMs to certain classes of people. This sets up a conflict between the rights the law grants to people and the means that they are allowed to employ to use these rights.

It is our belief that the law would be better and more consistent if it recognised that breaching a TPM isn't a problem, rather the problem occurs if the deprotected work is subsequently pirated, for which there are already legal remedies. This approach would recognise the rights of both the original rights holder and the purchaser.

Reasonable Circumvention

In conclusion, we believe that it is important that anti-TPM measures be available (e.g. DVD players that allow users to play legal DVDs from any region) to ensure that people can enjoy the rights that they have purchased. We further believe that owning anti-TPM equipment and circumventing TPMs for the right reasons should not be illegal in any way.

Recommendations

5. That ACTA should recognise that anti-TPM measures have a useful and lawful purpose.
6. That ACTA should insist that participating countries allow consumer rights-holders the right to create, buy and use anti-TPM software and devices if these are used for lawful purposes.
7. That ACTA should forbid the use of TPMs that limit the reasonable and customary rights of people to enjoy the use of the rights that they have purchased or otherwise legally obtained, unless the supplier also undertakes to provide unprotected versions when required.

Copyright Management Information

What enforcement measures should ACTA contain for remedying and deterring the removal or modification of copyright management information attached to, or embodied in, a copyright work?

Our Response

We support the right of rights holders to add CMI (Copyright Management Information) to their works. Unlike in the case of TPMs, this does not infringe the rights of purchasers in any way.

However, we see no reason that there should be a law against removing CMI. This is equivalent to someone removing the front pages from a book they own. We note that removal of this information does no damage to the rights holder and makes no difference to the copyright status of the work.

The New Zealand Copyright Act recognises this by saying that the motive of the person removing the CMI has to be taken into account – it is only an offence if you do it with criminal intent. As for TPMs, the removing of CMI is not an issue, it's the subsequent copying of the work that damages the rights holder.

Recommendations

8. That ACTA should not include enforcement measures concerning the removal or modification of copyright management information.

RELEASED UNDER THE
OFFICIAL INFORMATION ACT