No 16

Google

31 March 2010

Ministry of Economic Development
trademarks@med.govt.nz

Anti-Counterfeiting Trade Agreement - Invitation for submissions about intellectual property rights enforcement in the digital environment

Google appreciates the opportunity to provide further comments in relation to the Anti-Counterfeiting Trade Agreement (ACTA) digital environment provisions. These comments are supplementary to our earlier submission, dated 10 February 2010. Please take into account both these comments and our earlier submission.

As in our earlier submission, our comments relate to enforcement in the digital environment with a focus on copyright policy. If substantive aspects of trademark, patent or other intellectual property laws are implicated by the ACTA, we would appreciate the opportunity to comment on those as well.

We have set out our comments as responses to the questions posed in the consultation paper. We would be pleased to elaborate on or discuss any of these issues with you further.

1. **Liability of third parties for infringement**

The ACTA is an anti-counterfeiting, enforcement trade agreement. As such, it should not venture into issues of substantive intellectual property law and policy. Despite this, it appears that third-party liability in the digital environment is under consideration.

The application of an early 18th century field of law - copyright - to quickly evolving 21st century technological innovation is complex to say the least. The mere threat of disproportionate liability can significantly hamper legitimate innovative activity of great societal benefit. National legislative processes, incorporating input from all affected parties, are much better suited to addressing the implications to the full range of domestic stakeholders of regulating such a dynamic field than an international trade negotiation.

Moreover, once an international agreement like the ACTA is reached, it is exceptionally difficult to revise and update to keep pace with technology, given the number of countries involved. Google therefore believes that the ACTA, if concluded, should not have provisions on the Internet and digital environment, including third-party liability for Internet service providers.

If the ACTA negotiators do nevertheless seek to address digital environment issues, the New

Zealand Government should press for text that does not mandate any single approach, but rather allows member countries great flexibility in crafting solutions that are matched to national conditions and national objectives.

In addition, it is imperative that, if the ACTA does address third-party liability, it must also require robust safeguards (including limitations, exceptions and safe harbours) for Internet Service Providers (ISPs) and others in relation to infringements by those using their services or products. Liability standards must not be considered separately from relevant limitations and exceptions.

We also believe it is essential to bear in mind that there is no settled definition of third party liability at an international level. One party's doctrine, developed through its unique legal and economic situation, will not be a fit for all. And, as noted in our earlier submission, it is particularly inappropriate to base international law on a domestic legal doctrine that is the subject of ongoing litigation and considerable debate. Further detail on this point is provided in our earlier submission.

a. ***Safe harbours for ISPs***

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?

As discussed above and previously, we believe that the ACTA should not address substantive issues of intellectual property law, particularly in a rapidly evolving area like the digital environment. If, however, the agreement does, and provides for third party liability, it is important that the full balance of intellectual property law and policy be reflected, including limitations, exceptions and safe harbours. As such, the ACTA should include provisions requiring ACTA parties to provide robust limitations on third-party liability, including clear safe harbours for ISPs.

Limitations on third-party liability are imperative in ensuring that New Zealand remains a place where online innovation, creativity and free expression can thrive. Safe harbours and appropriate limitations and exceptions to copyright are essential to the operation of innovative online services. If ISPs – including hosting platforms, search engines, and other online platform operators - faced potential liability for their ordinary operations, or the wrongful use of their services by others to infringe copyright, that would be unjust and impractical, and it would essentially give right holders (RH) a veto over their ability to provide a platform for legitimate use and innovation.

In terms of activities that should be covered, any safe harbour provision should provide for limitation of liability for the full range of intermediary internet services. Any provision should be drafted in a technology neutral way that covers the current range of intermediary services and anticipates the ongoing evolution of those services. Also, it should state clearly that entities that

meet the safe harbour qualifications are not liable for monetary relief.

While requiring a baseline of limitations on liability and safe harbour provisions, any ACTA digital environment provisions should also provide countries with flexibility to develop and experiment with safe harbour regimes that are efficient and effective (for example notice-notice systems, whereby an intermediary must forward a properly made notice to an Internet user, have proved to be effective mechanisms).

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

There are many different types of ISPs, including hosting platforms, search engines, other online platform operators as well as those providing access to the Internet. Each of these types of ISPs operates in different ways in different circumstances. The nature of the service provided must be taken into account in the approach for safe harbours.

In relation to those providing access to the Internet, Google would be very concerned if there were any suggestion, by illustrative example or otherwise, that a condition for eligibility for the safe harbours were the implementation of a 'three strikes' type process.

As noted in our earlier submission, Google has been pleased with the public, consultative process that the New Zealand Government has undertaken in deciding how to implement the soon-to-be-repealed Section 92A and the new *Copyright (Infringing File Sharing) Amendment Bill* regarding the proposed requirements for an Internet access provider's response to allegations of infringement through peer to peer file sharing. This consultation process has led to important improvements in the process aimed at taking into account users' rights and due process. It has also highlighted that this is a delicate, complicated issue, with a range of important domestic interests at stake – further highlighting the risks of taking up these issues in an international trade negotiation.

Under any safe harbour regime, RHs should be expected to meet certain conditions – including meeting basic due process requirements that protect those who may be wrongly accused of infringing activity and that take into account the practical challenges that ISPs face in identifying and removing infringing material. While many legal systems provide RHs with ways to request the takedown of allegedly infringing material, checks and balances are necessary to protect lawful uses of copyright materials and to prevent abuse of the process.[1]

[1] For example, the U.S. system allows for counternotices, as well as lawsuits against the senders of takedowns who knowingly materially misrepresent that material is infringing. For a discussion and examples of erroneous takedowns, see, e.g., Jennifer Urban and Laura Quilter, 'Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act',http://mylaw.usc.edu/documents/512Rep-ExecSum_out.pdf, May 2006; Marjorie Heins and Tricia Beckles, "Will Fair Use Survive?"http://fepproject.org/policyreports/fairuseflyer.html, December 2005; Marjorie Heins and Laura Quilter, "Intellectual Property and Free Speech in the Online World: How Educational Institutions and Other Online Service Providers Are Coping with Cease and Desist Letters and Takedown Notices,"http://fepproject.org/policyreports/quilterheinsreport.pdf, January 2007; "Letter to Google and YouTube

To the extent that the ACTA provides for a particular notice-and-takedown system – which, as discussed above, Google thinks would be a mistake -- procedural requirements should be specified, including that:

- the complainant is the RH or the authorised agent of the RH. It is essential that only those with the relevant rights be able to issue a notice of alleged infringement.
- a notice of infringing content must meet agreed-upon standards, which at a minimum, would include clear identification of the allegedly infringing content by URL or other unique identifier, and a clear statement of the basis of the claim, including the country in which the law applies.
- the complainant should be required to provide a declaration that the information provided is true to the best of their knowledge, with penalties for false declarations.
- any notice which fails to meet minimum requirements should not create actual or imputed "knowledge" of allegedly infringing content for the ISP.
- the complainant should be subject to penalties for false or bad faith claims.
- users who created or distributed the content at issue should have the opportunity to challenge the removal.

b. ***Specifying when an ISP is liable***

We note that the consultation paper states that:
"An alternative approach to providing greater legal certainty for ISPs might be to include a provision requiring ACTA parties to ensure that civil remedies to compensate for damage resulting from infringing activities are available against an ISP when an ISP does not take appropriate measures to stop or prevent the infringing activity when, for example:
(i) it is technically possible for ISPs to take measures for preventing the infringement; and
(ii) the ISP knows or there is reasonable ground to know that the infringement is occurring."

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?

It is difficult to comment without the full context, however based on the information provided we believe that this alternative approach would raise serious concerns and would not better achieve

---

from McCain/Palin 2008 campaign regarding takedown of political speech on YouTube,http://www.eff.org/files/McCain%20YouTube%20copyright%20letter%2010.13.08.pdf, October 13, 2008; "Viacom: Fair use is what we say it is",*Wired Blog Network*,http://www.webmonkey.com/blog/Viacom:_Fair_Use_Is_What_We_Say_It_Is, August 31, 2007; "Boy dupes YouTube to delete videos",*The Sydney Morning Herald*, April 14, 2007.

the stated objective.

To begin, the proposed alternative approach is not a safe harbour or any other form of limitation on ISP liability – rather, it is a minimum condition under which liability must be imposed. Thus, it does not achieve the essential objective of ensuring that ISP liability is limited in a manner that creates the legal certainty necessary for ISPs to conduct their ordinary operations and provide legitimate services.

Additional, specific concerns with the language include that:

- The views of what are "appropriate" measures for ISPs to take will vary widely – how is this to be determined?
- What does it mean for something to be "technically possible"? Could it involve an assessment of whether a technology provider could have designed their system differently? This would create significant uncertainty, chilling technology development and investment.
- Even if a particular measure were found to be "technically possible", it may not be practical or efficient, and it may well entail undue burden on an ISP. As such, it might prevent or impede legitimate, non-infringing uses.
- An ISP will not generally know or have reasonable grounds to know about a specific allegation of infringement on its systems absent a formally adequate notice from the RH.

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

As noted, Google does not believe that the second approach outlined is appropriate. If the ACTA does address safe harbours, we believe national governments should be given full discretion about how to implement a system of limitations on liability; it must, however, at least require such limitations if it mandates liability.

2. Other matters

a. *Identifying infringing users*

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

A process enabling RHs to expeditiously obtain information from an ISP about the identity of an alleged infringer would be a new addition to civil procedure, limited to alleged online copyright infringements. Google believes that there are important user privacy issues at stake which need to be carefully considered before creating this unique avenue for RHs to uncover the identity of an Internet user based on allegations of infringement. The New Zealand Government appears to

acknowledge this, demonstrated by its careful consultation on the *Copyright (Infringing File Sharing) Amendment Bill.*

Google believes that if such a process is to be considered:

- there should be close judicial oversight, including a requirement for a judicial order for disclosure of a user identity;
- there should, at a minimum, be a requirement that a RH demonstrate reasonable grounds for an action against the alleged infringer before a judiciary can order disclosure of a user's identity; and
- there should be protections for ISPs in revealing users' details, for example, limitations of claims against ISPs by users.

b. ***Promoting cooperation between ISP 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 infringement of intellectual property rights taking place via the Internet? If so, how might a party promote such a relationship?

The opportunity to participate in the digital environment is important on a range of fronts, including ensuring that citizens have the opportunity to fully engage in the global digital economy and businesses can more effectively compete on the world stage.

The Internet is also a critical platform for RHs. It provides opportunities for innovative content services that improve legitimate access to content and address RHs' interests in the online environment. The most effective way to do so is to develop innovative content services that meet consumers' expectations and needs.

These new innovative services and cooperation mechanisms are for the private sector to develop, and indeed the private sector has been doing just that. In our view, it would be very difficult for governments to step into this process – which is constantly evolving as technologies and business models evolve -- at all, let alone through an international agreement. Moreover, such intervention is not necessary given the market is operating well.

For example, Google is proactive in working with RHs to manage their copyright online. For example, Google has invested substantial sums of money in the development of an automated content management system that is made freely available to enable RHs to manage their copyright material on YouTube.[2] Further detail about this system is available in the Annexure.

In addition, Google takes further steps to support the rights of both RHs and users. For example,

[2] For more information, see http://www.youtube.com/t/contentid

Google

it promotes consumer understanding of copyright, as evidenced by Google's well-developed policies and guidelines on copyright and copyright infringement, as well as the tips and articles offered to users on complying with copyright laws while using Google's products.[3]

These types of systems can be developed and thrive in market, and we urge the ACTA governments not to attempt to interfere in a natural development of new and efficient business models.

3. 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?

We refer to our comments in our earlier submission. As stated there, the ACTA should not require prohibition of circumvention of access control TPMs, without regard to whether such circumvention is related to infringement. Anti-circumvention laws related to access control TPMs may have nothing to do with infringement – which is the subject of the ACTA – and are often used in ways that hinder competition and innovation, as well as undermine the lawful use of content.[4]

To the extent TPMs are addressed in the ACTA, the agreement should not go beyond New Zealand law – ie it should be limited to devices or services that circumvent TPMs where the circumvention is tied to actual acts of copyright infringement.

We would be pleased to discuss any of the issues raised in our earlier submission or these comments.

Kind regards

Ishtar Vij
Public Policy and Government Affairs
Google Australia and New Zealand

[3] We would be pleased to provide more information on this.

[4] For example, the U.S. Digital Millennium Copyright Act's provisions related to access controls have been used in a number of instances to stifle legitimate activity. See EFF, "Unintended Consequences: Seven Years Under the DMCA,"*available at*http://www.eff.org/wp/unintended-consequences-seven-years-under-dmca.

Google

ANNEXURE

The YouTube copyright management system identifies matches between user uploads and copyright protected material and gives RHs the ability to maximise the use of their content according to their individual preferences.[5]

An example of this system in action is the 'JK Wedding Entrance Dance' video on YouTube.[6] By using the YouTube content management system for this video, the RHs have claimed and monetised the song, as well as started running Click-to-Buy links over the video, giving viewers the opportunity to purchase the music track on Amazon and iTunes. As a result, the RHs were able to capitalise on the massive wave of popularity generated by the 'JK Wedding Entrance Dance' video. In the last week of July, over a year after its release, Chris Brown's 'Forever' has again rocketed up the charts, reaching as high as #4 on the iTunes singles chart and #3 on Amazon's best selling MP3 list.

Below, we provide an overview of some of the tools developed by Google for the YouTube service, which protect RHs and inform users about the use of copyright protected materials:

- YouTube offers an automated notice and take-down tool which enables RHs to easily search for and identify videos on the site that contain their content, and promptly remove them with the click of a mouse.
- YouTube also uses technology that creates unique identifiers of files that are removed from YouTube for copyright reasons and prevents identical files from being uploaded to the site.
- YouTube informs its users about copyright and strongly discourages infringement (in a "Copyright Tips" section of the YouTube website). It also includes clear and prominent messages concerning rights ownership at the point that users upload user-created content, as well in its Community Guidelines, terms of use and via links to YouTube's copyright policies on every page of its web site.
- YouTube also provides a feature called "AudioSwap" enabling users to illustrate their original videos with music that YouTube licenses from music publishers and record labels. The purpose of this is to give YouTube's users easily accessible options for being creative, and use licensed music in their creations.
- YouTube Content Management Tools: YouTube provides technology to enable RHs to produce unique identifiers of their copyright protected audiovisual works. If such works are then identified, RHs are empowered by being able to decide what should be done with this content, including monetising it.

[5] For more information, seehttp://www.youtube.com/t/contentid
[6] http://www.youtube.com/watch?v=4-94JhLEiN0

Google

New innovative tools such as the ones developed by Google for YouTube are offering a way for users to legitimately access a wide range of content, and for RHs to protect their content, by identifying, managing access to it and, where they wish, monetising it. These types of tools and services can only be implemented if the regulatory framework allows for the necessary flexibility for new methods of cooperation between Internet intermediaries and RHs to develop.