No. 9

Colin Jackson - Submission on ACTA – March 2010

1. This submission is provided in response to the invitation for submissions about intellectual property rights enforcement in the digital environment released by Minister Power in March 2010.

Background

2. I am Colin Jackson, an independent technology consultant and commentator. I have wide experience as an IT practitioner and IT policy specialist. I am a founder and a past president of InternetNZ, the public-good not-for-profit body that runs the core of the Internet in New Zealand. I am a member of the New Zealand Computer Society and an Information Technology Certified Professional. The views expressed in this submission are my own.

3. My comments on ACTA below relate to those of its provisions that affect the Internet, its suppliers and most importantly its users. I make no comment on physical counterfeit goods. However, I observe that the agreement is misleadingly named, since its title makes no mention of digital information. This may have exacerbated the general view that there is poor transparency around ACTA.

4. MFAT and MED have advised that any changes to New Zealand law due to ACTA will be limited to enforcement of matters which are already unlawful. This is hard to be certain of before the agreement is concluded, however if true it would be wrong to say that this could not affect New Zealanders' daily lives. An example of an activity that is unlawful and widespread but not enforced is jay-walking.

Overall Comment on ACTA

5. Thank you for this opportunity to provide a submission on ACTA in advance of the Wellington negotiating meeting. I last wrote a submission on ACTA in August 2008, when I stressed the importance of the Internet to New Zealand and the real risks of damaging it by enforcing ISP liability on matters over which they have no control. I remain extremely concerned that this provision is still on the table.

6. The fundamental principle that needs to be respected in ACTA is that the rights of the great majority – that is people who use the Internet or digital media – should not have their interests damaged in pursuit of a global enforcement regime for copyright holders.

7. According to the World Internet Project, 83 per cent of New Zealanders are Internet users. The unmediated communications that the Internet provides are reshaping our economy and our society. We use it for everything from banking to entertainment, from seeking news to seeking a partner. We use it to attract tourists – our second-biggest export earner – and we use it to sell them airline tickets. Increasingly, government services are provided over the Internet, in some cases exclusively. Government uses it to track and disseminate the customs and quarantine regulations that our agricultural exporters need to do their business. And our burgeoning high-tech sector relies on an effective and improving Internet to compete with the rest of the world. It is crucial that we would avoid damaging the Internet and innovation that it encourages in order to advantage one industry sector at great cost to everyone else.

Transparency

8. Efforts to improve the transparency of the ACTA negotiations are welcome. I appreciate the lengths that MED and MFAT have gone to in briefing the New Zealand public in the last few weeks.

9. However, it is unacceptable, in the view of a large number of people including the European Parliament, that an agreement with such a potentially wide-sweeping effect be negotiated in secret. It is hardly surprising that speculation about the contents of ACTA have ranged far and wide. I urge New Zealand to do all in its power to allow all sectors of society and the economy to comment on the draft texts and to achieve a mechanism that is seen to balance the interests of copyright-holders with those of ordinary Internet users.

Questions in Invitation to Submit

Safe Harbours for ISPs

10. The overriding principle here has to be that ISPs are not threatened with liability over things they cannot control, or that they can only control by cutting off customers or functions from the Internet.

11. This term "safe harbour" suggests that the default position of ISPs is that they are liable unless they can show that they are in a safe harbour. This is an unfortunate way of looking at things, to say the least, since ISPs are common carriers like a postal delivery service. We do not seek to hold a courier liable for delivering an unlawfully-copied CD and we should extend this to the ISP that provides digital equivalent. Ideally our Copyright law would be rewritten to clarify this status. However, absent a major rewrite of copyright, the "safe harbour" concept is more likely to bring legal certainty for ISPs, provided that the safe harbours provided are sufficiently general to permit Internet operation and innovation.

12. There is an frequently-quoted misapprehension that ISPs have the technical capability to detect and foil copyright infringement. It is a technical fact that ISPs cannot determine with certainty what their customers are doing on the Internet. Even if ISPs were to implement an intrusive and privacy-invasive regime of inspecting all their customers' Internet traffic, they would not be able to see the contents of any communications protected by encryption (such as Internet banking). Encryption is necessary for electronic commerce and is becoming increasingly common for ordinary Internet traffic. For instance, Google's Gmail service now encrypts traffic to its users by default.

13. This blindness to traffic contents is the result of a deliberate design decision taken in the early days of the Internet, known as the "end-to-end principle". This is fundamental to the Internet's architecture. It states that the Internet simply moves bits from one location to another with no understanding of their significance. This principle is key to the Internet's usefulness, because it allows new services to be developed and implemented across the Internet without the need to negotiate with ISPs. This has happened many times in the Internet's history and will doubtless keep happening. The World Wide Web, Twitter, Skype and even email are services which have been designed to run through the Internet, but are not part of the architecture of the Internet itself.

14. Meaning is imputed to Internet traffic only by the people at each end of the flow of data, using the devices with which they connect to the Internet. For example, when accessing a web page, the user's web browser (such as Internet Explorer or Firefox) displays the text and graphics forming a web page which makes sense to the user, but to an ISP the Internet traffic involved consists of bits flowing to and fro in a protocol commonly used by web traffic which may or may not happen to be encrypted. ISPs could in principle sometimes make reasonable guesses about the meaning of Internet traffic they are passing, but these guesses would not always be accurate and in many cases no guess would be possible.

15. Simply asserting that ISPs are aware of their users' traffic is therefore wrong, and a poor basis for policy-making. Forcing ISPs to accept liability will cause them to refuse to handle traffic they cannot know to be non-infringing. This would have the effect of preventing any new services from appearing on the Internet. Taken to extreme, this would effectively prevent the participatory model of communications that the Internet has promoted, rendering the Internet little more than a large cable TV system where customers consume content provided by a few large licence-holders.

16. A further issue is that an ISP is not well placed to determine the merits of any claim of copyright infringement by a putative copyright holder. There have been many cases where claims are found to be invalid. Google, for instance, states that 37% of the claims it receives prove to be invalid. Most New Zealand Internet connection providers are far less well-resourced than Google. Safe harbours need to shield ISPs from liability for hosting disputed material until infringement is proven. In New Zealand, S92C of the Copyright Act makes ISPs liable if they do not immediately remove material they host on behalf of customers in response to an assertion of infringement made by a third party – this can have a dangerously chilling effect since it allows people to have material removed from the Internet on the basis of an unsubstantiated allegation. ISPs should have a safe harbour from unproven allegations under ACTA, as they should in New Zealand law, which should be amended on this point.

17. Finally, it is important not to succumb to arguments to the effect that a whole class of technologies (e.g. peer-to-peer filesharing) is should be made de facto illegal by being excluded unconditionally from ISP safe harbours. There are substantial non-infringing uses for peer-to-peer, and, more generally, new services and technologies on the Internet always challenge existing assumptions about how the Internet works.

18. To summarize: the whole approach of safe harbours for ISPs is unfortunate, since it leads to a mentality that "everything that is not permitted is forbidden" which is antithetical to innovation, but this may the best we can do in the short term. ISPs cannot technically determine the content of their customers' information flow, and enforcing liability on them will effectively break the Internet and destroy its ability to allow new services. The approach should be to provide sufficient safe harbours so that ISPs are liable only where they can be proven to have deliberately facilitated copyright infringement in a way that does not have substantial non-infringing uses, such as knowingly hosting a public archive of unlicensed copyright material.

Specifying when an ISP is Liable

19. The driving principle should be that ISPs must not be held liable for things they cannot control.

20. I distinguish between material that an ISP hosts (i.e. makes available on the Internet) on behalf of a customer, and material that customers host for themselves on servers that are not owned by the ISP. It is generally possible for ISPs to remove infringing material that it hosts. It is not possible for an ISP to remove material its customer hosts on servers it does not own without effectively cutting that customer off altogether. This would in general be a disproportionate measure that would potentially affect more people than just the alleged infringer, such as other businesses on the same connection, or other people in the same physical residence.

21. It is reasonable that an ISP be liable for knowingly making available unlicensed copyright material. This would apply, for instance, where the ISP hosted a web page that contained an unlicensed work. This liability would have the effect of facilitating a rapid removal of unlicensed material on direction by the copyright holder. Because of the power it gives a putative copyright holder to control material that may in fact not be copyrighted, it is essential that this provision be balanced with a penalty for vexatious or reckless assertions of infringement.

22. However, if an ISP is providing Internet connectivity to a customer who is alleged to have committed an act of infringement, the ISP should not be liable provided it facilitates communication between that customer and the person who claims to hold the infringed copyright.

23. Any agreement needs to reflect this distinction and provide for liability only for items that are within ISPs' control.

Identifying Infringing Users

24. Assertions of copyright infringement are just that – assertions. Until claims have been weighed by a court there is no good reason to allow a putative copyright-holder access to the identity of an accused infringer, and valid privacy reasons not to allow it.

25. Where a copyright-holder has concerns that its interests are being damaged significantly, it can always apply to a court for an urgent injunction.

Promoting cooperation between ISPs and right holders

26. This is a matter for the parties concerned. It is not generally seen as a role of government to promote "mutually supportive relationships" between one industry sector and another. It is unclear what the government could do to achieve this if it wanted to. Government attempts to force a negotiation between these groups in early 2009 failed (this was part of the discussion around S92A of the Copyright Act that never came into force). An international agreement requiring governments to do this would likely result in wasted resources and embarrassment.

Technical Protection Measures

27. The problem here is around unlicensed use of copyright material, not about TPMs (which are known outside legal circles as DRM, for digital restrictions management). It would be far better to address unlicensed use directly rather than the mechanisms used to attempt to enforce it.

28. There are some very significant problems with DRM:

i. DRM is being used to suppress legal rights. There are many examples of established "fair use" rights being prevented by DRM. In New Zealand we do not have fair use, but we do have specific rights such as format-shifting of audio works, e.g. copying music from a CD or a paid-for download to an MP3 player for personal use. DRM can be and is being used to prevent format-shifting.

ii. DRM is platform-dependent. Each implementation of DRM is tied to specific hardware or software. For instance, Wellington City Libraries offers audiobooks that can only be played on Microsoft Windows-based computers. This has the effect of damaging competition and innovation, and angers users who find that equipment and content they have acquired won't work with their computers.

iii. DRM causes user frustration. A good example of this would be the DVD region code. DVD region coding is not protected by law in New Zealand and multi-zone DVD players are available, yet coded DVDs still cause frustration and lost hours as people try to exercise their rights to play the DVDs they have purchased in computers, other DVD players, cars etc.

iv. DRM requires an unhealthy level of control over users' computers. This allows DRM suppliers potentially full access to everything a user does on that computer. Perhaps the most egregious example of this was the Sony / BMG rootkit incident 2005, in which Sony inserted software into some of its audio CDs which took control of users' computers and set up a mechanism for Sony to peruse the contents. This software was exploited by viruses on the Internet, which led to the thousands of people who had purchased these CDs and played them on their computers having their computers infected.

29. There are signs that the time of DRM may be passing. Many online music stores such as Apple's iTunes that formerly used DRM now sell their music unencumbered, mainly for the reasons listed above. Instead, online stores insert "watermarks" – a hidden record inside the music file so that the purchaser can be identified. This serves as a mechanism to deter copyright infringement.

30. To summarize: there should be no requirement for nations to introduce a law to deter the circumvention of DRM, because circumvention is sometimes necessary or desirable for reasons unconnected with copyright, such as to facilitate access by blind people or to exercise legal rights..

Copyright Management Information

31. Removing copyright management information does not change the fact of copyright. Copyright materials with their copyright signs removed or altered are still copyright materials. To put it another way, the problem that ACTA seeks to address is unlicensed use and distribution of copyright material, not altering the labelling.

32. If a provision to the effect that CMI cannot be altered is included in ACTA, this will provide an opportunity for content providers to integrate the CMI with other provisions that users would not wish for such as mechanisms for logging their identity and location, and the users would not legally be able to anything about it.

33. To summarize: content management information is not the point and could introduce unintended consequences. Its protection should not form part of ACTA.

Conclusion

34. The ACTA process is the biggest single current threat to the continued development and usefulness of the Internet. I remain of this view even after examining the various unauthorized texts in circulation. It is essential that all those negotiating the agreement gain an understanding of the technology involved, rather than accepting the self-serving assertions of groups that regard the Internet's existence as a threat.

35. I reiterate my thanks for the opportunity to submit. I would be happy to answer questions or provide a face-to-face briefing on request.

Colin Jackson

5.9(2)(a)