



BUDDLE FINDLAY

FEBRUARY 2012

Legal update on Information and Communication Technology.

IN THIS ISSUE

- [Torrenting of private photos prevented](#)
 - [Australian cloud computing guidelines](#)
 - [SOPA and PIPA - Implications for New Zealand websites](#)
 - [Government launches its government cloud programme](#)
 - [AstraZeneca v IBM](#)
 - [Megaupload shutdown signals risks in the cloud](#)
-

TORRENTING OF PRIVATE PHOTOS PREVENTED

In the UK case of *AMP vs Persons Unknown*, [2011] EWHC 3454 (TCC), an unnamed British woman (AMP) has obtained an injunction to prevent anyone from distributing explicit images of her on the internet, including by using bittorrent technology. The images of AMP, and of her family and friends, were stored on her mobile phone. Some of the pictures were sexually explicit and intended for her boyfriend's eyes only. The phone was stolen in 2008 and images were uploaded initially to a Dutch internet site and later to a popular, Swedish-based bittorrent site. The images, identifying the woman by name, were downloaded an unknown number of times but by a comparatively small number of people, mostly based in the UK and the wider EU.

AMP sued to enforce her right under the European Convention on Human Rights to respect for her private life and for relief from harassment. The London Technology and Construction Court held AMP had a reasonable expectation of privacy in relation to the images given the circumstances in which the photographs were taken, the nature and purpose of the intrusion caused by the theft and distribution of the photographs, and the effects on AMP. The court also held that AMP's rights were not outweighed by the downloaders' right to freedom of expression (which includes the right to receive and impart information without interference). The right to freedom of expression is also protected under the EU Convention on Human Rights. This case suggests that the misuse of personal information on internet, including using bittorrent, may be more "regulatable" than previously thought.

AUSTRALIAN CLOUD COMPUTING GUIDELINES

The Australian Government Information Office has released a guideline on cloud computing. It provides some useful guidance on the legal issues worth considering when considering entering into cloud arrangements. It can be found [here](#).

SOPA AND PIPA - IMPLICATIONS FOR NEW ZEALAND WEBSITES

For many, encountering Wikipedia's blacked-out landing page in mid-January was the first that they had heard of SOPA (Stop Online Piracy Act) and PIPA (Prevent Real Online Threats to Economic Creativity and Theft of Intellectual Property Act*), two US legislative measures aimed at preventing foreign websites from enabling or facilitating infringement of US copyright.

SOPA and PIPA were introduced into the US Congress (in the House of Representatives and the Senate respectively) in 2011 and were intended to give the US Justice Department jurisdiction to prosecute owners and registrants of websites, wherever in the world they might be located. Key elements of the proposed legislation include:

- The ability to send a notice of the alleged violation and intention to proceed with further action to registrants and owners of foreign websites if those websites:
 - are available to US users, and
 - commit or facilitate commission of an infringement of US copyright
- The ability to target intermediaries (such as ISPs, advertisers, search engines and payment network providers) as a way of shutting down access to an infringing site. For example, if "Website X", run by a New Zealand business, was found to be infringing US copyright, the US Department of Justice could serve notices on Google (to prevent Website X showing up in search results), on Paypal (to freeze any finances generated by Website X), on advertisers (to cease making advertisements available to Website X) and, finally, on Website X's ISP (to block access to the site)
- The ability of rights owners to then commence an action for limited injunctive relief provided consent to US jurisdiction is given and
- New bureaucratic appointments in the form of "Intellectual Property Attaches" to be assigned to a US embassy or diplomatic mission in each geographic region (such as East Asia and the Pacific).

Both the US Senate and the House of Representatives have halted progress on the bills following widespread criticism and staged internet blackouts by web giants like Wikipedia and Reddit. However, despite 400,000 telephone calls to Congress and many politicians withdrawing their support for the legislation, key proponents of the bills are still intent on getting the bills (or some reincarnation of them) through.

How would all of this affect New Zealand businesses? If these or similar bills are enacted, we could see the long arm of the US Justice Department stretch all the way down-under, thereby substantially altering the face of the world wide web. If that does eventuate, New Zealand businesses will need to be vigilant not only to ensure that their websites do not infringe US copyright, but also to ensure that they contain no links to other potentially infringing websites. As to whether these particular bills will pass into law? We can only suggest that you watch this (cyber) space.

* This name of course spells "PROTECT IP". Unfortunately, that acronym has since been discarded in lieu of the more wieldy but slightly less poignant "PIPA".

GOVERNMENT LAUNCHES ITS GOVERNMENT CLOUD PROGRAMME

Recently the Department of Internal Affairs (DIA) posted a Registration of Interest (ROI) notice on GETS (the government's electronic tendering site) inviting suppliers to contribute to the development of an indicative business case for the government's adoption of cloud computing services.

DIA expects that a business case will be completed and presented to the ICT Ministers by the end of April 2012. If the business case is approved, all core public service agencies would be expected to adopt the Government Cloud Programme as soon as they can practically do so and other wider state agencies, such as Crown entities, DHBs and schools, would be invited to join. The government is interested in the adoption of cloud computing services because of their potential to reduce capital investment in ICT and reduce associated on-going operating costs. DIA has stated that its syndicated contract for Infrastructure as a Service (IaaS) will continue to be a key component of any future cloud based model adopted by government. The DIA press release can be found [here](#).

ASTRAZENECA V IBM

The recent UK case of *AstraZeneca UK Limited v International Business Machines Corporation [2011] EWHC 306 (TCC)* concerned a dispute relating to the exit provisions in a Master Services Agreement (MSA) for IT infrastructure services between IBM and AstraZeneca. The parties disagreed as to the scope of IBM's contractual obligations to provide post-termination assistance.

The Technology and Construction Court ultimately upheld AstraZeneca's interpretation of the services that IBM must provide. The case is very fact specific, but it illustrates the importance of considering parties' obligations post-termination. Exit management is often over-looked in the rush to get a contract finalised. However, the best time to negotiate such matters is when drafting the contract, rather than following termination when the parties are often no longer on good terms.

In an IT contract, exit provisions should include as much detail as possible about the services to be provided on exit and any materials, information or resources which must be provided to the customer to successfully transition to a new provider. It is also important to include clear details of the length of time that the transition services will be provided for and how much those transition services will cost (or mechanisms for determining these details).

MEGAUPLOAD SHUTDOWN SIGNALS RISKS IN THE CLOUD

The file storage and viewing websites run by Megaupload were shut down by the US Justice Department in January 2012 alleging copyright infringement. New Zealand based executives of the company, including Kim Dotcom, were arrested by New Zealand authorities and face extradition to the US on charges of racketeering, money laundering and copyright crimes. Megaupload is reputed to have had some 50 million users, some of whom stored legitimate copyright works with Megaupload, such as personal images and videos and confidential documents. Megaupload's servers were hosted, according to the US Justice Department, by two third party hosting businesses, Cogent and Carpathia.

Megaupload users were obviously concerned about whether they could get their files back after the shutdown. According to Wikipedia, on 20 January 2012 the US Justice Department stated that "It is important to note that Mega clearly warned users to keep copies of any files they uploaded" adding that "Megaupload.com expressly informed users through its Frequently Asked Questions (FAQs) and its Terms of Service that users have no proprietary interest in any of the files on Megaupload's servers, they

assume the full risk of complete loss or unavailability of their data, and that Megaupload can terminate site operations without prior notice". Subsequently the US Attorney's Office has stated it has no ongoing access to the "Mega Servers" and that they are not in the actual or constructive custody or control of the US Government. The alleged hoster Carpathia has also since denied it has access to any of Megaupload's servers or information and has advised users to "contact Megaupload".

This leaves Megaupload users in a very difficult position. The US Government says it has no rights to access the files and at least one of the alleged hosters says it has no access to the files. Finally, the users' contract with Megaupload says that if you uploaded a picture of your kids to Megaupload you ceased to have any rights to that file and if the file gets deleted, that is your problem. If you are considering storing valuable files "in the cloud", it is vital that you find out who actually stores the files, ensure that you have ongoing legal rights to the files and consider what the process would and should be if something disrupts the cloud service.

[Back to top>>](#)



STEVE NIGHTINGALE

Partner

DDI: 04 498 7312

steve.nightingale@buddlefindlay.com



PHILIP WOOD

Partner

DDI: 09 357 9385

philip.wood@buddlefindlay.com



ANDREW MATANGI

Consultant

DDI: 04 498 7315

andrew.matangi@buddlefindlay.com



AMY RYBURN

Senior Associate

DDI: 04 462 0904

amy.ryburn@buddlefindlay.com



AISLING WEIR

Senior Associate

DDI: 09 363 1346

aisling.weir@buddlefindlay.com



ALLAN YEOMAN

Senior Associate

DDI: 09 363 1029

allan.yeoman@buddlefindlay.com

BUDDLEFINDLAY

Buddle Findlay produces a range of topical legal updates. If you would like to subscribe to other legal updates, please [CLICK HERE](#).

If you have any questions on issues covered please contact the sender.

This article is provided for general information purposes only and not as legal advice.

[CLICK HERE](#) to unsubscribe if you no longer wish to receive information and communication technology email legal updates from Buddle Findlay.