



## iiNet: Lessons for New Zealand

On 20 November 2008 34 television and film companies sued Australia's second largest ISP, iiNet, for copyright infringement by its customers. The case has just concluded in the Australian Federal Court in Sydney.

The Australian Federation Against Copyright Theft (AFACT), which ran the case for the TV and film companies (we have an equivalent NZFACT here), argued that iiNet should be held liable for its customers use of the BitTorrent peer to peer protocol in downloading illegal copies of songs and movies. AFACT argued that by not preventing its customers' illegal downloads, iiNet had authorised its customers' copyright infringement and was therefore equally liable. iiNet argued that it was not its job to monitor, interfere with or judge its customers' activities (it forwarded the infringement notices it received from AFACT to the police).

The law in Australia and New Zealand on authorisation of copyright infringement is similar so what does the case mean for us here? This question is very relevant now as we decide what to do about section 92A – the repeat infringement provision that the recording and movie industries hope will be the killer app for peer to peer in New Zealand. ICT law expert, Rick Shera of Lowndes Jordan, followed the case for *NBR* and makes some observations.

### Evidence

AFACT collected evidence against iiNet over 59 weeks. It did so primarily by using a European company called DtecNet to upload infringing material from iiNet's customers using BitTorrent. That then supposedly gave AFACT the internet protocol (IP) addresses of the customers' computers, which in turn enabled it to send infringement notices to iiNet as the ISP for those IP addresses.

In some weeks, iiNet was sent over 1,000 such notices. It was alleged that over 100,000 infringing songs or movies were downloaded. No New Zealand ISP could cope with that number of notices even under the less labour intensive notice forwarding system proposed under the revised s92A.

AFACT's counsel conceded that an ISP faced with such a deluge might only be expected to actually deal with 25% of the notices, but even that would be an insurmountable task for a New Zealand ISP.

The collection and reliability of IP address evidence was questioned by iiNet. Justice Cowdroy's findings on this will be highly relevant here since DtecNet is also used in New Zealand. IP address evidence has been questioned in other jurisdictions also.

### Cost

The iiNet case took over 4 weeks to hear. iiNet has reported that the case has cost it more than A\$4 million and that does not include the time cost and distraction for its personnel involved (its CEO, Michael Malone, was on the stand for 3 days). Presumably AFACT has spent a similar amount.

### Termination based on accusation alone

At the heart of AFACT's case is its view that ISPs have a responsibility to kick infringers off the internet. As an affiliate of the Motion Picture Association in the US, it subscribes to the *three strikes or graduated response* school of thought. ISPs should respond to notices from copyright owners by sending warnings and then terminating customers' internet accounts without the need for Court scrutiny of those notices. NZFACT subscribes to the same view as does the Recording Industry of New Zealand (RIANZ), which represents the major record labels.

By not terminating, AFACT argued that iiNet was condoning its customers' infringements and should therefore be held liable for them.

In New Zealand, the *guilt upon accusation* suggestion caused public outcry in early 2009 with the blackout campaign and continues to be generally rejected.

## ISPs as gatekeepers

AFACT argued that ISPs make money out of traffic over their systems and therefore have a responsibility to police or *gatekeep* the internet. It regards the internet as a means by which infringement takes place and therefore a privilege that must be monitored, restricted and, if necessary, removed. It even wants ISPs themselves to close down if they do not comply. iiNet and most ISPs argue that they are mere conduits – they do not know what is being transmitted over their systems anymore than an electricity company knows what its electricity is being used for. Nor, they argue, should they be required to actively spy on their customers to find out. Not only would this be an invasion of privacy but it would be prohibitively expensive (a cost which would have to be passed on to customers) and would degrade performance at a time when increasing bandwidth capacity and speed is a national priority.

It has to be asked also whether we want unaccountable commercial ISPs to be policing the internet and making decisions for us about what does and not get through. Conversely, in North America, the focus is on making sure that ISPs remain neutral as to what material they transmit.

A decision in the iiNet case is not expected until next year. It will be eagerly awaited in Australia, New Zealand and indeed around the World as the struggle over copyright on the internet continues.

This article was first published in the National Business Review on 11 December 2009.