From the editors...

New technology, faster broadband, the proliferation of smart phones and new online services are giving rise to a host of legal challenges considered in this issue.

Jessica Gurevich and Capucine Hague consider the 'Bring Your Own Device' or BYOD phenomenon, a recent trend whereby companies allow or require employees to use their own phones, laptops or similar devices for work purposes. They discuss key factors and legal implications that companies need to consider in formulating a BYOD policy.

Katrina Cavanough, the winner of the 2012 Student Essay Prize, considers the implications of modern technology and ever-increasing broadband speed for copyright protection, and the potential for ISPs to play a gatekeeper role in the fight against piracy of copyright content following the 2012 High Court decision in *Village Roadshow Pty Ltd v iiNet.*

The difficulties facing traditional notions of copyright in the digital age are further explored in the context of online video streaming services in separate articles written by Victor Lei and Jesse Gleeson. These articles highlight the uncertainty surrounding the questions of whether streaming copyright content is an infringement of copyright, and whether the provision of streaming and recording services (for instance, of free-to air television) constitutes copyright infringement.

In her article 'Sub-licences – Underestimated and Overlooked?', Anne Petterd considers recent UK case law that considered a tricking software licensing question, namely, whether a sub-licence can continue to exist once the head licence under which it was given falls away. A recent ruling of the England and Wales High Court suggests that under certain circumstances, a sub-licence may continue on-foot notwithstanding the termination of the head-licence.

Daniel Thompson, David Ng and Isaac Lin

have a comprehensive plan in place risk security breaches and loss of confidential or commercially sensitive information through lack of employee awareness of appropriate measures that they may need to take.

Key recommendations

1. Balance interests – BYOD isn't simply about protecting company information, it's also about respecting employee privacy.
2. Invest time in creating and implementing a comprehensive use and security policy.
3. Make BYOD official – don't just tacitly approve or tolerate employees using their own devices.

Considerations when developing a BYOD policy

Accessible types of data

Employers should consider whether they will restrict the data which their employees have access to on their own devices. There is a significant difference between allowing employees to access company communications (email, voice calls and SMS messages), and facilitating access to software, platforms, resources, documents and raw data. Corporations should consider whether the benefit of allowing employees access to the data in question from their own devices outweighs the associated risks. A clear policy should be adopted regarding the types of data available to employees on their own devices, and may be customised depending on the individual employee. Perhaps more importantly IT infrastructure should be geared to enforcing these restrictions and IT staff will need to understand the company's position on access to information from personal devices so that they can effectively implement those measures.

Companies will also need to consider whether there are additional legal or regulatory restrictions on accessing or using certain sensitive data, for instance medical records, financial details and personal information. Some jurisdictions limit offshore storage of certain information without the corporation specifically retaining a measure of control. In addition to the existing risks a corporation may face from its own usage of cloud based platforms and storage solutions, an employee's personal use of a public cloud based solution on their BYOD device may place the corporation in breach of certain regulatory obligations.

Data does not have to be stored directly on an employee's device. Allowing employees to store copies of data on their own device creates a risk of data leakage, and may also mean that the company does not have access to the most up to date version. Data also becomes vulnerable to loss or destruction if the device storing it is lost or destroyed. It is often preferable to store data and applications on a remote server or cloud storage system which is accessed over a secure internet connection (preferably VPN). However, as noted above, measures should be taken to ensure that only devices which have been vetted have access, for instance by restricting the IP addresses able to access the server.

Licensing

Corporations will inevitably be subject to certain licensing restrictions for certain software and services. Often enterprise-wide software will be licensed on a per device basis. In such circumstances, BYOD activities may inadvertently exceed the number of authorised and