From the editors...

Against potentially favourable cost and convenience considerations, cloud computing raises privacy, security, performance and regulatory issues. In their article, *Cloud Computing: the Legal Dimension*, John Gray and Vinod Sharma address key aspects of those issues. In particular, they consider some of the emerging legal and practical issues faced by those seeking to embrace this new technology, flagging the need to make express provision for the ownership of intellectual property rights. The authors hint at the complexities involved in using a storage medium offered in and accessed from multiple jurisdictions.

Spam, a by-product of one of the now well-established technologies, continues to annoy and present threats despite attempts to outlaw its sending under certain circumstances. As with some other electronic communications, limiting spam by requiring potential recipients to opt-in or opt-out is a key feature of Australian and American legislation. Kayleen Manwaring examines the relative effectiveness of those alternate strategies as well as other aspects of legislative attempts to control spam in her article, *Canning the spam five years on: a comparison of spam regulation in Australia and the US.*

Courts are not often called upon to construe software licences. In a previous edition (July 2009) Colin Bosnic reviewed a number of Australian court decisions concerning IT software failures and commented on the low number of reported and unreported cases. Accordingly, it is not surprising that there are very few intermediate and final appeal court decisions. Recently, in *Software AG (Australia) Pty Ltd v Racing and Wagering Western Australia* (2009) 175 FCR 121, the Full Federal Court considered whether the statutory entitlements in ss 47C and 47F of the *Copyright Act 1968* (Cth) to make back-up copies of computer programs and the provisions of the software licence permitted the making of a back-up copy which was kept at a "warm" disaster recovery site. Martin Squires and Susan Lee examine how the Court's business-like approach to interpretation assisted to resolve an ambiguity in the software licence.

Contributions are welcomed

If you would like to contribute an article, case note, book review, or any other material relevant to computers and the law, please contact us at editors@nswscl.org.au. A brief style guide appears at page 15 of this edition and a number of suggested topics for anyone needing some inspiration appear at page 4. We are very interested in hearing from you, so sharpen up your quills ...

Jeanette Richards, Vinod Sharma and Martin Squires

Continued from Page 1

Cloud based solutions place greater control of data in the hands of service providers than traditional solutions. Given that all of the processing is performed in a remote location, the user organisation may not have access to the software which performs the processing. Where the cloud solution is designed to perform a business critical function, user organisations may feel vulnerable to the cloud services provider.

Certain laws and regulations govern a person's use of particular kinds of data, and these may impose legal obligations on both a cloud services provider and a user organisation. For example, obligations regarding the handling of personal information are imposed by the *Privacy Act* and *National Privacy Principles*. However, it would be unwise for a user organisation contemplating a cloud services arrangement to rely solely upon such legislative protection for the safeguarding of data.

Because the actual possession of data is outside the user organisation – indeed, the data will be held in the ubiquitous, shared environment of the Internet – it will be imperative to ensure the contract with the service provider spells out which party owns the data, confers strong rights on the user organisation to retrieve copies of the data, and imposes strict obligations on the service provider to protect the security of the data. It may even be appropriate for a user organisation to insist on the secure segregation of its data, perhaps on physically isolated storage media, from that of other users.

A further consideration is that a cloud computing arrangement may result in data being subject to regulations in the jurisdiction in which the data are physically stored or processed. For example, anti-terrorism laws confer on many foreign governments wide-ranging powers to access and retrieve copies of respect of data. It would be prudent to investigate this when contemplating a cloud services arrangement.

Performance issues

Cloud computing is delivered by the Internet, that amorphous, multipartite "network of networks" accessed by millions of clients each moment of the day. Consequently, a cloud computing service is theoretically subject to greater risks of disruption and delay than traditional computer usage models reliant upon dedicated infrastructure. For example, peaks in the volume of network traffic passing through either a cloud service provider's network, or through the user organisation's internet service provider's network, may affect the quality of services provided to the user organisation via the cloud.