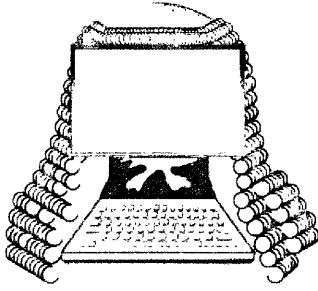


# COMPUTERS & LAW

Journal for the Australian and New Zealand Societies  
for Computers and the Law



Editors: Jeanette Richards, Vinod Sharma and Martin Squires

ISSN 08117225

Number: 76

December 2009

## Cloud computing: the legal dimension

*John Gray and Vinod Sharma*

**John Gray (Partner, HWL Ebsworth)** has over 18 years experience as an intellectual property and technology lawyer in Australia and overseas. He is the national leader of HWL Ebsworth's Technology, Media and Communications group.



**John Gray**

**Vinod Sharma (Associate, HWL Ebsworth)** is an intellectual property and technology specialist with qualifications in IT and law. He has previously worked as a technology professional and as in-house legal counsel to both IT customers and vendors. He is currently completing a Master of Law and Management at UNSW and AGSM.



**Vinod Sharma**

*John and Vinod joined HWL Ebsworth in July 2009.*

At its simplest, cloud computing is computer processing delivered as a service over the Internet.

As cloud based solutions enter the enterprise technology market as a mainstream service, the opportunities for user organisations to rationalise their technology infrastructure by decreasing localised processing and simplifying system requirements around access to the “cloud” – that is, the Internet – are attractive.

The time has arrived to consider some of the associated legal issues.

### What is it?

Cloud computing is a new label given to a concept that originated in the early years of this century. It involves using the platform of the Internet for the provision of software, infrastructure and related services as a combined service offering.

The key idea behind cloud computing is that users will be provided with highly scalable access to software and related services without having to contemplate, let alone install and manage, the technology infrastructure that is ordinarily required for a user to access software in a networked environment.

This is likely to result in the growth of “pay per use” applications where users pay for use of software as if it were a utility service. It will mean not having to purchase long term licences of software or maintain the operating environments required to effectively run such software.

### Key legal and commercial issues

The rise of cloud computing as a model for computer usage may require you to consider a variety of significant legal and commercial issues.

### In this issue

<i>John Gray and Vinod Sharma, Cloud computing: the legal dimension</i>	1	<i>Martin Squires and Susan Lee, Case note - Software AG (Australia) Pty Ltd v Racing and Wagering Western Australia (2009) 175 FCR 121</i>	12
<i>Kayleen Manwaring, Canning the spam five years on: a comparison of spam regulation in Australia and the US</i>	5		

### **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](mailto: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.

This is a problem that is being addressed incrementally, through the evolution of intelligent network technology which will drive improved quality of service. Meanwhile, for a user organisation reliant upon computer processing to carry on its business, ensuring the continual availability of the cloud computing service and its performance to a certain standard will be essential, particularly in circumstances where the solution is of business critical significance.

Strategies a user organisation should follow to minimise the risk of performance issues include:

- implementing rigorous service level provisions in the contract with the services provider; and
- performing due diligence from the outset to ensure the reliability of the service provider.

In addition, support and maintenance structures in many cloud based solutions may be different to the traditional models which organisations have become accustomed to. Increased centralisation may mean that traditional models of "in-house" support and maintenance will move into a shared, centralised model in the cloud. For certain business critical cloud services, dedicated support and maintenance customised to the individual user organisation's needs will inevitably have a place in the cloud services market.

### **Dependency**

Cloud computing transactions will inevitably raise a variety of legal issues which will require careful attention in contracts between user organisations and service providers.

For many organisations, information technology is critical to commercial success. Divesting the operational and management control of IT from such organisations into the cloud will result in significant commercial dependency on the cloud services provider. Not only may a cloud service provider have control over software, but also over all of the infrastructure and platforms that facilitate access to the software. If there is a fault in the cloud service provider's systems, it is unlikely that the user will have any access to be able to rectify it itself, let alone any visibility into what is causing such fault.

Cloud engagements need to include mechanisms which incentivise the service provider to perform yet ensure business continuity for the user organisation in the event of a fault either in the software being provided, or in the platforms or infrastructure supporting such software. Furthermore, not having the applicable software installed in-house, a user organisation should consider whether access to software source code may be necessary.

It will be important for user organisations to avoid becoming "locked" into proprietary cloud solutions without effective exit mechanisms, and being exposed to variations in service quality or pricing.

Robust contractual arrangements will play a role in addressing some of these issues. Clauses concerning

pricing variations and transition-out arrangements will become an area of focus in negotiations of cloud computing services contracts. Transition-out provisions should deal with how the parties intend to handle the migration of data held in the cloud back to the customer in a non-proprietary format which facilitates transitioning to a new service provider.

In cloud solutions, a user organisation's business processes might be engineered around effective use of the cloud service to maximise commercial efficacy. Changes to the service being provided – such as the implementation of updates to the system – may have significant consequences for the user organisation, and will necessitate careful management. User organisations might wish to obtain a guarantee from the service provider on a certain set of features to alleviate concerns about forced changes to business processes arising out of future new releases and upgrades.

Contracts for cloud based solutions, like any other, should include measures to mitigate the risks for customers migrating to the cloud. The importance lies in how such agreements achieve a commercially pragmatic outcome which has the effect of alleviating some of the significant risks faced by user organisations.

### **Intellectual property**

Intellectual property will inevitably be developed by user organisations using cloud solutions. This could be as simple as a document created on word processing software hosted on the cloud, or as complex as a new scientific model using combined high speed processing and software technology accessed via the cloud. The ownership of intellectual property rights should be covered in the services contract so as to protect the interests of both parties.

Often, the parties will need to consider the geographical location of the technology infrastructure supporting the cloud solution, to ensure compliance with any local laws dealing with the ownership of intellectual property rights. Any assignment of intellectual property over materials created in the use of the cloud solution should be drafted to comply with all formal requirements of the laws of the host jurisdiction. Further, user organisations should retain a right to veto changes to the physical location of cloud technology.

### **Concluding thoughts**

Before it became fashionable to refer to the Internet and its various components as "the cloud", selected elements of cloud computing had already been embraced by user organisations. Now, for the first time, integrated cloud based solutions are entering the market as a mainstream service.

Certain legal and commercial issues that would be familiar to practitioners assume greater importance in cloud computing: data protection and security; performance and functionality; support; transition-out; intellectual property; and jurisdictional concerns.

Merely recycling existing contractual templates for this new commercial computing model will be a recipe for disaster.

Don't get lost in the cloud - think through the issues and implement a contract that appropriately covers off the risks.

### **NSWSCL WEBSITE UPDATE**

The process for updating the NSWSCL website is currently underway. Following an exhaustive requirements and evaluation process, we now see the completion of the new website in the near future. The benefits of the new website for both members and subscribers will be:

- an updated, user friendly interface with improved navigation
- online renewals and details update for both members and subscribers
- online payments
- online discussion boards for "Computers & Law" issues
- access to past editions of the Computers & Law Journal
- seamless content contribution by authorised members
- searches of the Journal and other site content
- event calendar and bookings
- extensive links to other legal websites

In addition, a complete membership application is being implemented that will make the administration of all Society tasks more efficient and timely.

### **CONTRIBUTIONS TO THE JOURNAL**

Do you have something to say about law and computers, information technology, the internet or telecommunications? Have you read any interesting cases or books about computers and the law lately? Is there an issue you think would interest your fellow members of the Australian and New Zealand Societies for Computers and the Law?

The Editors encourage all readers to contribute to the Journal. The Editors welcome contributions of any length (from a short case note or book review, to an in-depth article) on any topic relevant to computers and the law.

If you have an article you wish to contribute, or even an idea for an article you would like to discuss, please contact the Computers and Law Journal Editors at [editors@nswscl.org.au](mailto:editors@nswscl.org.au).

By way of example, following are some topics that could form the basis of an article:

- the Australian Government's review of e-commerce legislation (*Electronic Transactions Act 1999* (Cth) and its state and territory equivalents) and whether Australia should accede to the UN Convention on the Use of Electronic Communications in International Contracts 2005
- the Australian Government's review into the Government's e-security policy, programs and capabilities
- the detection of fraudulent emails
- the litigation against iiNet alleging copyright infringement
- the Australian Government's review of options for reforming the existing telecommunications regime