Stormy Weather Ahead?

The Rise of Cloud Computing

By Michael Davis and Alice Sedsman**, Adelta Legal*

The Internet has transformed so much of our daily lives – from communications to news, information, recreation and entertainment. The latest revolution in Internet use is cloud computing. Most of us have already unknowingly joined that revolution and the social and legal implications are only starting to be understood.

Cloud computing email services such as Gmail or Hotmail are in widespread use. Personal social-networking services such as MySpace and Facebook also utilise cloud computing. However the real revolution is in the impact of cloud computing on business computing. Cloud computing applications are starting to have a profound effect on the way businesses operate by reducing or eliminating the need for businesses to invest in hardware and software.

By providing software applications and data storage as a service, cloud computing providers take responsibility for the electronic records of businesses. This centralised model reduces, if not eliminates, the need for businesses to purchase and maintain their own servers, individual software licences, support staff, and floor space for computer servers. Other benefits include the reduction of power costs and the consequent reduction in carbon emissions, at least for the business client.

Cloud computing is blind to international borders. In practice, a person's data may be stored in and delivered from huge server facilities or 'server farms' located in any region of the world.

Cloud computing has been dismissed by sceptics as a passing fad; the next 'dot.com bubble'. However, since the emergence

Continued over page...

Stormy Weather Ahead?

...Continued from previous page

ERD Court on YouTube

Even the Courts cannot escape the fact that technology rules the world and increases the ability to reach a wider audience.

In what is believed to be a first in Australia, South Australia's Environment Resources and Development Court (ERD Court) has published five instructional videos on YouTube.

The move was made because of the high number of unrepresented litigants using the court and supplements information available over the counter and on the CAA website. The videos and other additional information are also available from the registry in DVD format for use on computer.

The publication of the material on YouTube recognises a potentially new and emerging group of court users.

The videos don't offer specific legal advice and are intended as guides only.

The Senior Judge of the ERD Court, Judge Trenorden said the use of YouTube was in line with her view that the courts should be making use of modern forms of communication in a form that people actually use.

"It explains what we are, what we do, how we do it and how the court can be accessed when needed, including what is expected of litigants in court."

A link has been placed on the CAA website (www.courts.sa.gov.au) look on the ERD Court home page for "videos"). On YouTube (www.youtube.com) key into the search engine: ERD-how to.

of Amazon Web Services, Google Apps, Microsoft Office Live and IBM Blue Cloud, cloud computing has commanded a new respect as a phenomenon that is changing the shape of the IT industry. The staying power of cloud computing has been bolstered through the uptake of cloud computing services by major corporations such as Coca Cola Enterprises, Nokia and The New York Times.[1]

The present popularity of cloud computing services can be attributed to marketing campaigns that promise end-users low charges for data storage facilities and free access to computer programs such as word processing, bookkeeping and collaborative networking. However, as we shall illustrate, the lack of end-user control over the computing services and their own data has significant legal consequences.

One of the greatest conveniences of cloud computing is its worldwide accessibility. Being Internet based, cloud computing allows end-users to access and modify their data from any suitable device with Internet capabilities. Access is available from any location where Internet connection is available with high enough bandwidth.

However, as cloud computing is Internet based, an obvious risk to end-users is unscheduled system outages. Businesses can make alternative arrangements when outages are scheduled for in-house system maintenance and upgrades, but when an Internet server goes down without warning, all access to critical applications and data could be lost for the duration of the outage.

Even large cloud computing providers experience unscheduled outages from time-to-time. In February 2008, Amazon suffered an outage that lasted for four hours. On 14th May this year, Google experienced technical problems which brought down its own homepage and caused its search site, email, YouTube and Google News to perform sluggishly or to become unavailable to some users. Although this lasted for only two hours, the worldwide impact was profound.[2]

At best, an outage might cause a minor disruption to a business. At worst, it may mean a huge loss of business, missing of deadlines and permanent loss of data.[3] The thought that business records could be lost is alarming, especially when most contractual terms of use for cloud computing systems exclude or limit liability for loss of business in such circumstances. Of further concern is the uncertainty of technical support offered by provider companies. When cloud computing systems glitch, end-users are often unable to do anything but wait for the functionality of the systems to be restored.

Direct technician support is commonly made available to end-users for an additional fee, but considering the enormity of cloud computing systems, this support may be inadequate in practice. If all end-users of a cloud computing service lost access simultaneously, support lines would probably be overwhelmed.

Even foreseeable risks, such as the damage or destruction of all of a person's information stored by the cloud computing provider, have not yet been adequately addressed. While most terms of use assure end-users that recovery plans are in place for any such disasters, the timeframe and costs for recovery are not specified.

The ability of end-users to transfer their data to other providers or back to their own server at will and without charge is also uncertain. Similar questions of access arise in the event that the provider stops providing the service. The terms of use for Google Apps Premier Edition provide for the return of end-users' data on request. However, no timeframe or cost basis is ascertainable and there is no guarantee that the returned information will be in a portable format.

End-users who pay for cloud computing services face particular risks if they fail to pay their accounts within time. Google and Microsoft warn that in such circumstances the services will be suspended at first instance and terminated if the default continues. Termination is in itself problematic. For instance, on termination the end-user may lose all control over his or her data and there is the risk that the data will be permanently deleted by the provider.

The Rise of Cloud Computing

By Michael Davis and Alice Sedsman**, Adelta Legal*

"The word 'free' when used in advertising should ring alarm bells to our profession. Unexpected conditions are often couched in rarely-read terms of use."

Most standard forms of agreement for cloud computing services currently fail to address these issues.

The word 'free' when used in advertising should ring alarm bells to our profession. Unexpected conditions are often couched in rarely-read terms of use. One well publicised example is that of Google's free Gmail service. In its Privacy Policy, Google advises end-users that the Gmail service includes advertising 'based on the ... content of messages and other information related to your use of Gmail.'[4]

Cloud computing providers are the gate-keepers to the data that end-users place on their networks. Concerns have been expressed that, without scrutiny, providers may be tempted to covertly sell end-user personal information to market and consumer profiling corporations. Most countries have some form of privacy law to regulate dealings with the personal information of customers. However, the effectiveness of these laws can decrease the further from home the information is stored.

Generally, privacy laws protect two categories of information: personal and sensitive information. Personal information is that which can be used, either independently or accumulatively, to identify an individual. Sensitive information is a further category of personal information which usually receives additional legal protection. Sensitive information is information that could be used to discriminate against an individual, such as information about an individual's racial or ethnic origin, political affiliations, religious affiliations, philosophical beliefs, sexual preferences or practices, criminal record or health.

Privacy laws generally require prior notice to be given to individuals before their personal or sensitive information is collected and used by a third party. However, the requirement of prior notice is often only loosely fulfilled, especially when notice is given through links from an organisation's website homepage. The Google Gmail service is a prime example.

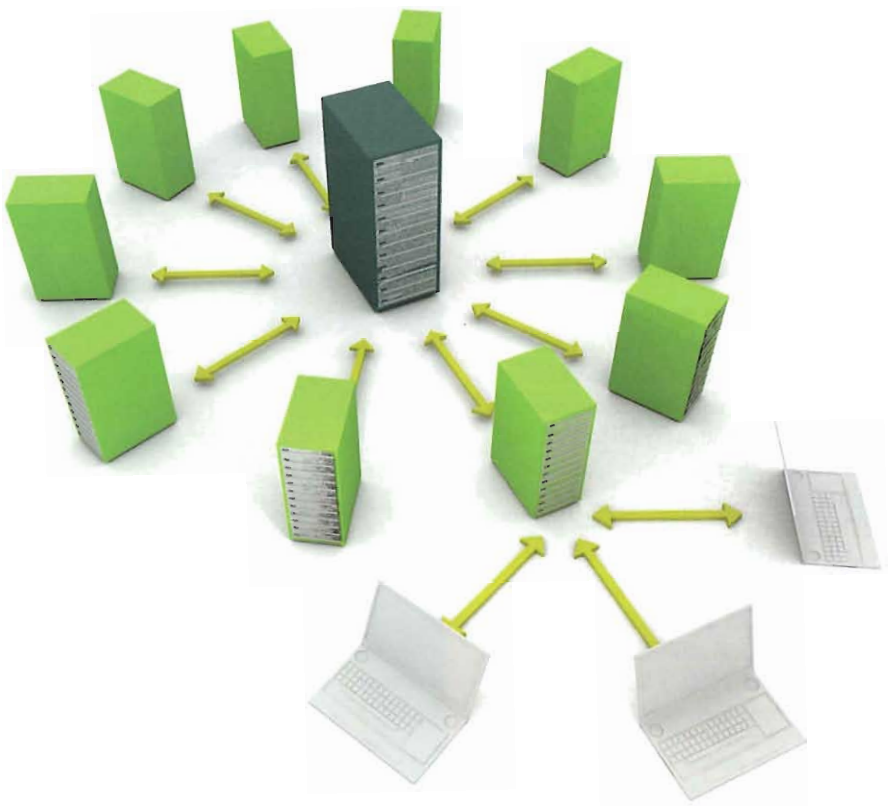
Privacy protection legislation aims to ensure that individuals give informed consent to the collection of their personal and sensitive information. Google relies on the public availability of its privacy policies to provide notice of collection to individual end-users, but in reality few people will ever read these policies.

In our commercial world we have come to accept the phrase 'caveat emptor' (buyer beware) as good policy. However, it is not necessarily an appropriate principle in a field as sensitive as personal privacy rights. Some uses and collection of personal and sensitive information clearly need to be prohibited, no matter whether constructive or actual notice has been given to individuals. Getting users to actively 'opt in' to individual terms of use that affect their privacy should also be considered as a protective measure.

Continued over page...

Stormy Weather Ahead?

...Continued from previous page



Aside from intentional misuse of personal information, privacy can be innocently eroded by human and system errors. In 2001, pharmaceutical company Eli Lilly accidentally disclosed the email addresses of 669 Prozac users.[5]

As cloud computing continues to attract clients in the banking, telecommunications, government, education and health industries, the need for vigilance over personal information of end-users increases. In developing countries the number of industries turning to cloud computing as an affordable alternative to in-house IT infrastructure is growing exponentially and includes organisations that house sensitive personal records.[6]

The protection and enforcement of individual rights to privacy is complicated by the trans-border flow of data that is at the heart of cloud computing. Every time an end-user inputs data into the cloud, information is transmitted from that end-user's home country. Every time end-users log into their accounts, their information may pass through any number of unknown countries as it is retrieved and transmitted back to the end-user's computer. In most instances end-users will never know where their personal information is stored, let alone which country's privacy laws apply and how to invoke them.

Many cloud computing terms of use are silent on the issue of how long an end-user's information will be stored for and how it can be destroyed or de-identified. There is a current debate as to whether Australian law is adequately protecting rights to privacy. The Australian Law Reform Commission recently reviewed Australia's privacy laws and reported that some businesses (namely database operators, detective agencies and providers of telecommunications goods and services) pose a high risk to the confidentiality of personal information.[7] These businesses generally hold vast quantities of information (often sensitive in nature) about individuals and routinely carry out privacy intrusive activities. In Australia, approximately 94% of businesses were exempt from the application of the *Privacy Act* in 2007.[8] The ALRC is recommending changes that would see all businesses subject to uniform privacy laws.

The trans-border nature of cloud computing complicates jurisdictional issues. For instance, if an end-user resides in Australia, but his or her information is stored in America and China, the governments of both those countries may monitor the contents of that end-user's cloud computing account. In such circumstances, the non-national end-user is unlikely to be informed of, let alone given an opportunity to oppose, such privacy intrusions.

In its terms of use, Google endeavours to make reasonable attempts to contact the end-user when a third party attempts to access end-user data.[9] However, sometimes it will fall on the cloud computing provider to resist the proposed incursions of privacy on behalf of the end-user. To its credit, Google recently resisted an attempt by the FBI to access millions of Google end-user logs by subpoena.[10] This attempt to access end-user records highlights the dangers of storing sensitive information in another legal jurisdiction.

The importance of securing end-user data is reaffirmed daily, with the ever escalating rate of cyber crime. Corporate espionage costs business millions of dollars every year. It is now common practice for businesses to ban their employees from using live cloud computing networking applications such as Facebook in order to reduce the risk of employees leaking confidential company information.

In addition to wider concerns about privacy, security and access to data, end-users of cloud computing systems should beware of terms of use that limit or remove their usual legal rights, particularly those terms that pertain to intellectual property and choice of law.

When end-users upload their data to cloud computing providers, they generally expect to retain the copyright and other intellectual property rights in that data. However, in some instances, cloud computing providers

The Rise of Cloud Computing

By Michael Davis and Alice Sedsman**, Adelta Legal*

have undermined these expectations by issuing end-user terms of use that grant the provider a licence to use end-user data without charge.[11]

It is common for cloud computing providers to insert jurisdiction and choice of law clauses into their end-user licence agreements.[12] These clauses usually purport to be a binding nomination of a specific court in a specific place to hear any dispute that may arise out of provision of the services. The nominated court is usually selected for its proximity to the operations of the company that drafted the contract.[13]

Choice of law terms aim to override domestic laws that grant citizens specific contractual rights. Cloud computing providers can protect their own interests by electing the most sympathetic forum to determine claims. The consequences for end-users are clear: the application of foreign laws and the hearing of matters in foreign territories seriously impede the ability of end-users to bring or defend claims against cloud computing providers. The legal and ethical accountability of the providers is thereby diminished.

This article has only touched on some of the legal issues that are likely to affect businesses and private end-users. As is the case with so many emerging technologies, there are gaps that need to be filled before the legal system is adequate to the international dimension and technical realities of cloud computing.

"Many cloud computing terms of use are silent on the issue of how long an end-user's information will be stored."

**Michael Davis is a partner of Adelta Legal, a boutique Adelaide commercial law firm. He has wide experience in advising clients in the information and communications technology sector. He is a Faculty member of the International Space University and until recently was Chair of the Advisory Board of the Institute of Telecommunications Research at the University of South Australia.*

***Alice Sedsman originally studied journalism before turning to law in 2005. She graduated from Flinders University with an Honours Degree in Laws and Legal Practice in mid 2009 and now works as a solicitor with Adelta Legal. She is also a graduate of the Mobile Enterprise Growth Alliance incubator program. Alice has a particular interest in technology commercialisation and is a member of the South Australian committee of the Australian Interactive Media Industry Association.*

1 Arnold, E. Get your head out of the clouds. Retrieved from http://www.infotoday.com. Lyons, D. Newsweek, Retrieved from http://www.newsweek.com/id/166818. Fitzgerald, M. Microsoft puts its head in the cloud. Retrieved from http://www.fastcompany.com/magazine/130/microsoft-puts-its-head-in-the-cloud.html

2 Google gridlock affects millionsí. Retrieved from http://www.news.com.au/adelaidenow/story/0,22606,25487704-5006364,00.html

3 In 2008 MobileMe, a cloud computing initiative of Apple designed to synchronise data stored in Macbooks, iPhones and iPods, crashed. A small percentage of MobileMe end-users who had paid for the service instantly lost every email they had ever sent or received.

4 Google Inc. Gmail Privacy Notice. Retrieved from http://mail.google.com/mail/help/intl/en/privacy.html

5 US Federal Trade Commission. Eli Lilly settles FTC charges concerning security breach. Retrieved from http://www.ftc.gov/opa/2002/01/elililly.shtm

6 The Economist (London) ëThe long nimbusí. Retrieved from http://www.economist.com/specialreports/displaystory.cfm?story_id=12411864&CFID=39572738&CFTOKEN=45450076

7 Australian Law Reform Commission. (2007). Review of Australian Privacy Law: Discussion Paper No 72

8 Ibid

9 Google Inc. (2008f). Google Apps Standard Edition Agreement. Retrieved from http://www.google.com/apps/intl/en/terms/standard_terms.html

10 McCullagh, D. Google to feds: Back off. Retrieved from http://news.cnet.com/Google-to-feds-Back-off/2100-1030_3-6041113.html

11 In 2008, Google experienced customer backlash when a drafting oversight resulted in clauses, which granted Google intellectual property rights over all data uploaded by end-users, being inserted into the end-user licence agreement for its new Internet browser, Google Chrome. Google altered the offending clause within 24 hours and Google Chrome end-users now enjoy retention of their intellectual property rights.

12 See for example Google Terms of Service. Retrieved from http://www.google.com/accounts/TOS?hl=en

13 For Australian users of Microsoft Office Live, the courts of Singapore have jurisdiction. For users of Google Apps, the courts of Santa Clara, California are given jurisdiction. The laws to be applied are those of Singapore and Santa Clara County respectively.