Innovation

ARTHUR COX

EXPECT EXCELLENCE

MAY 2010

Technology Group Briefing

Cloud Computing & The Law

Cloud Computing in the News

Microsoft's CEO Steve Ballmer has described cloud computing as a US$3.3-trillion opportunity. The British government said earlier this year that it was planning to cut £3.2 billion from its annual IT bill of about £16 billion by creating its own cloud platform. Locally, Minister for Communications Eamon Ryan has identified cloud computing as one of the key driving forces towards the creation of a smart economy, while the IDA's recently published "*Horizon 2020*" report regards access to and deployment of cloud solutions in Ireland as fundamentally important pre-conditions for the delivery of foreign direct investment in the coming decade. It makes sense for Ireland to be at the forefront of innovation in this space, given that we host an enviable list of the top internet corporations in the world.

What is Cloud Computing?

There is no universally accepted definition of cloud computing. A simple description is that cloud computing is computing via the internet, whereby shared resources, software and information are provided on-demand, much like public utilities such as electricity or gas. Other definitions expand on the three delivery models that exist (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS) and Cloud Infrastructure as a Service (IaaS)), and the four deployment models (private cloud, community cloud, public cloud and hybrid cloud). Some commentators dispute certain of these characteristics, in particular the concept of public-v-private clouds. Whilst the exact definition might be open to debate, there are two well-established principles to bear in mind when considering the issue:

1. the idea of sharing resources via web-based technologies is not new (for example web-based email accounts such as Gmail, Hotmail and social networking sites such as Facebook have for some time ticked all of the boxes for the cloud computing model); and
2. the true potential of cloud computing in terms of its application to business has not yet been realised, with many analysts putting multi-billion euro sums on the amounts that can be saved by replacing traditional IT infrastructure with cloud-based applications.

In other words, and like many internet innovations, the scale of actual take-up of cloud services is racing ahead while lawyers and legislators consider the legal implications.

Why the current movement towards cloud computing?

There are a number of significant benefits to cloud computing, including the following:

1. **Savings on IT spend:** This is perhaps the biggest driving force for many who are embracing the cloud. Cloud computing, and utility-based billing, will enable businesses to pay for computing as a service on an "as-needed" basis, rather than the traditional model of having to match or exceed demand at all times in terms of local resources.

This document contains a general summary of developments and is not a complete or definitive statement of the law. Specific legal advice should be obtained where appropriate.

Earlsfort Centre, Earlsfort Terrace, Dublin 2, Ireland | **tel:** +353 (0)1 618 0000 | **fax:** +353 (0)1 618 0618 | **email:** dublin@arthurcox.com | **web:** www.arthurcox.com

2. **Flexibility:** Cloud computing improves the ability of a business to quickly, and without significant cost, reposition itself in terms of infrastructure and demand. A major challenge under traditional IT models has been coping with peak demand and avoiding outages, whilst at the same time not over-spending on resources.
3. **Location Independence:** Cloud computing enables access to systems remotely.
4. **Security:** Whilst some argue that the risk of pooling data means that data breaches will prove more catastrophic, others point to the fact that pooling resources also enables the service providers to introduce more stringent security controls that are usually beyond the costs of individual businesses. They also point to the fact that many high-profile data breaches involve the theft or loss of physical media such as USB keys while cloud services will reduce the need for such physical media.
5. **Environment:** Pooling IT usage in modern and efficient data centres should reduce the carbon footprint of the IT industry, helping businesses to comply with energy regulations.

What are the Legal Issues?

Whilst much of the focus to date from a legal perspective has been on data privacy and security (and these are discussed below), a number of other considerations apply to cloud computing. These issues include the following:

1. **The Parties:** In contrast with more traditional outsourcing models where the service provider is readily identifiable and restrictions are usually put on the sub-contracting of services, the cloud can be dark at times, making it difficult for users to see who they are dealing with, who is storing and processing their data and where. Also, even if all the service providers are identifiable, issues of privity of contract may arise where obligations have been sub-contracted to a third party. As with any outsourcing arrangement, it is critical to the cloud customer that all service providers are identifiable, and accountable for their services.
2. **Flexibility:** Cloud services are still at a relatively early stage of development and little has been done to address the challenge of different technologies and standards developing which are not easily interchangeable or interoperable. Customers therefore need to pay particular attention as to whether services they purchase are compatible with their in-house systems as well as those services they buy in from third parties.
3. **Open Source:** Open source software is seen as being critical to the development of cloud computing. There is a common misconception that open-source software means "free" software. This may not always be the case, and there are often very real restrictions on the use of such software in a commercial context. It is critical to be aware of this before using open source software.
4. **Business Continuity:** As with any IT outsourcing arrangement, customers should consider at the outset what protections they will require to transfer the service to a third party should the need arise. For example, will there be a transitional phase to assist in the transfer of the service? Should there be an escrow arrangement in place? Will data be returned without further charge? "Standard" terms and conditions from cloud providers will often seek to exclude or restrict cooperation on the transfer to a new service provider, leaving the customer exposed on the expiry or termination of the contract.
5. **Governing Law:** It is not unusual for the service provider and the customer to be in different jurisdictions, and naturally therefore questions arise as to the applicable governing laws and which courts will enforce those laws. This may impact on a number of other matters, for example there may be mandatory provisions of local law that apply to data protection matters or the enforceability of exclusions or limitations of liability. Both the customer and the service provider need to consider this carefully so as to ensure the contract terms are enforceable.
6. **Unfair Contract Terms:** Service providers in the cloud will usually insist (in the first instance at least) on using their "standard" terms. These terms tend to be very one-sided, sometimes excluding all meaningful remedies for the customer, including in the case of data loss or service failure. In some jurisdictions, standard or non-negotiated terms may be unenforceable in certain circumstances if they are not reasonable, even in the case of business-to-business contracts (for example, the Unfair Contract Terms Act 1977 (**UCTA**) in the UK). Whilst there is no direct equivalent to the UCTA in Ireland, there may be consumer protection provisions that will apply to the customers of the business engaging the cloud service provider. These, and the applicable governing laws, should be considered before engaging any cloud service providers.

Data Protection in the Cloud

Cloud computing raises data protection compliance considerations by virtue of personal data being stored on servers in the cloud, as an alternative to such data being stored on an organisation's own computer network. Set out below is a high-level outline of the some of the fundamental data protection issues to be considered by any customer thinking of investing in a cloud solution for their business.

1. **Relationship between the Customer and Service Provider:** Data protection compliance provides a particular challenge for customers seeking to move to web-based solutions offered by the cloud computing model. The relevant law in Ireland is the Data Protection Acts, 1988 and 2003 (the "**Acts**"), which are largely based on European Union Directive 95/46/EC, with the Acts and Directive being enforced and

administered in Ireland by the Data Protection Commissioner. The Acts apply to "personal data", broadly defined in the Acts as data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller. The rules set out under the Acts apply to data controllers and data processors, with the former being the party who either alone or with others controls the contents and use of personal data, while the latter simply processes personal data on behalf of the data controller.

Generally the customer purchasing a cloud computing solution for its business will be the data controller in respect of the personal data processed as part of that solution while the provider of the cloud services/solution will be the data processor, although this situation will not always be clearcut. Data controllers are required to observe the fundamental data protection principles and related rules on processing, transferring or disclosing personal data under the Acts; hence being a data controller carries with it substantial legal responsibilities. On the other hand, unlike data controllers, data processors have a more limited set of responsibilities which primarily concern the obligation (with the data controller) to keep personal data secure from unauthorised access, disclosure, destruction or loss. In the context of the above structure, it is vital that the contractual arrangements between the parties for the provision of the cloud services properly allocate risks and responsibilities, e.g. regarding the respective security obligations of the parties, given the potentially drastic consequences of a data security incident.

2. **Security of Data:** Customers need to obtain concrete assurances (backed up by enforceable contractual remedies) from service providers that personal data processed and stored in the cloud is maintained safe and secure from unauthorised access, disclosure, destruction or accidental loss. In deciding what level of security is appropriate, the Acts requires the customer, as the data controller, to have regard to:

   (a) the nature of the personal data in question and the harm that might result from unauthorised use, disclosure or loss of such data; and

   (b) the state of technological development and the cost of implementing security measures.

   The security obligations under the Acts apply in particular to the transmission of personal data over a network, with guidance from the Data Protection Commissioner on this issue noting that "*this is understandable, since this type of transmission involves particular security risks that must be guarded against. Most obviously, there is the danger that the transmission could be intercepted by a third party*".

   Cloud solution providers may attempt to resist providing customers with binding and enforceable contractual assurances as to the quality or availability of their service and be reluctant to accept any significant liability in relation to service failure. However, as data protection law requires service providers to provide secure cloud services, customers should insist on dependable, reliable and secure cloud services from the provider, even where this may impact the pricing of the solution on offer. Furthermore the customer, as the data controller, must satisfy itself that the cloud solution provider, as the data processor, has suitable technical security and organisational measures in place and that it is adhering to these security measures (and that similar standards are maintained if personal data are disclosed to a sub-contractor).

3. **Data Exports:** EU data protection laws also impose restrictions on the export of personal data outside the European Economic Area (EEA), unless such country to which it is exported ensures an "*adequate level of data protection*". Special conditions must be met before transferring personal data outside the EEA, where the importing country does not have an EU-approved level of data protection law (and notably some important trading locations, such as the United States, do not enjoy this level of approval). While the data subject's consent will legitimise such a transfer, obtaining consent is not always a practical solution. The result is that most data controllers or customers address this requirement through reliance upon one of the sets of European Commission approved model form clauses for transfers or, in the case of transfers to the US, by requiring the US entity to be "safe harbor" certified. A further challenge posed by cloud services is that it is often impracticable to determine precisely where personal data have been transferred "in the cloud", which increases the challenges in adhering to these data transfer rules. Furthermore, service providers will often view compliance with the transfer requirements as solely the customer's responsibility.

4. **Applicable Data Protection Law:** By their nature cloud providers will use trans-border infrastructures to enable them to provide services as efficiently as possible. While the cloud solution offers obvious cost and structural benefits, issues arise if the solution is structured in a manner that renders the personal data processed as part of the cloud solution potentially subject to the laws of the various jurisdictions in which it is processed. Compliance can be further complicated where different jurisdictions have inconsistent data protection laws (most notably outside the EEA). In regulated areas such as financial services there can be specific restrictions under national laws governing how companies can outsource key business functions.

5. **Key Questions:** The following initial questions regarding data protection compliance should be considered by the customer and service provider when negotiating a potential cloud-based solution:
   (a) What kind of data will be processed and stored in the cloud?
   (b) Where will the data be processed and stored (e.g. where are the servers located)?
   (c) What measures are in place to keep the data safe from loss or unauthorised access?
   (d) Will the data be transferred to other locations and, if so, how will cross-border data transfers be undertaken in compliance with applicable data protection laws?

Conclusion

The parties should consider the issues above at an early stage with the aim of ensuring their contractual arrangements in relation to the cloud solution adequately address both legal obligations and their commercial needs, including for example data security, interoperability and business continuity. Typically before signing up to a cloud solution the prudent customer will have checked that the provider of the cloud solution has the technology and/or capability to properly provide the systems and services required. However a customer seeking to do business with the provider of a cloud solution will, ordinarily, have little scope to perform any significant investigation of the cloud infrastructure to ascertain whether adequate safeguards are in place. As a result it becomes crucially important for a customer to have robust contractual terms in place with the service provider to address the key risk areas, e.g. setting out the allocation of responsibility and risk in the event of a security breach in the cloud resulting in the loss of, or damage to, data of the customer.

While there have been some well-publicised examples of companies and public sector organisations being reluctant to embrace cloud solutions for fear of the legal implications, in truth the legal issues are not insurmountable and can be managed with proper prior diligence and, most importantly of all, with a balanced and well-drafted contract.

Further Information

For further information, please contact one of the following Arthur Cox lawyers:

Colin Rooney
Associate, Technology Group
tel: +353 (0)1 618 0543
colin.rooney@arthurcox.com

Emmet O'Grady
Associate, Technology Group
tel: +353 (0)1 618 0541
emmet.ogrady@arthurcox.com

or your usual Arthur Cox contact.