

Cloud computing in the public sector: risks and reward

Philip Nolan and Oisín Tobin examine the legal problems cloud computing presents and explore potential solutions

Cloud computing represents the latest phase in the evolution of information technology. Like most new technologies, it has engendered controversy and debate. Evangelists claim that it represents the start of cheap and ubiquitous computing; sceptics assert that it is no more than a passing trend, and one that poses considerable dangers to users.

But what exactly is cloud computing? What are the risks? Is cloud computing suitable for government? This brief article considers these questions from a legal standpoint.

What is “cloud computing”?

At its core, cloud computing allows a user to get the benefit of powerful computer infrastructure without paying the capital cost of purchasing such hardware and software.

Under a traditional approach to IT procurement, the buyer pays an upfront cost to purchase the necessary computer hardware and software. For large bodies, such as government departments or agencies, this usually takes the form of buying powerful, but expensive, computers called servers. Along with the upfront capital cost, the buyer also needs to budget for the storage, upgrading and maintenance of the hardware purchased, not to mention licence fees for software to run on such servers.

Cloud computing is based on the idea that computer power, software and memory are commodities, like electricity or gas, that can be purchased only when needed.

Companies, known as “cloud providers”, operate large “server farms”, which are essentially buildings full of powerful computers. Under a cloud computing arrangement, the cloud provider rents this computing power to its customers. Users can buy processing power or memory storage from a cloud provider and upload or download information to the cloud provider via the internet.

Under this arrangement, the user avoids paying any of the upfront costs traditionally associated with IT procurement. Rather, the user pays a set fee based on its use of the cloud (i.e. for the software and computer power used).

In addition, a large number of smaller



Philip Nolan



Oisín Tobin

IT companies, many of them Irish, have begun to use the cloud as a platform to sell software to end users. For example, an IT company may decide to provide online account management software to businesses. This company could host this online service “on the cloud”, i.e. using space on a server farm. Businesses that use the cloud in this manner are usually termed “end user service providers”.

The legal risks: Problems and solutions

The slow adoption of cloud based solutions by the Irish public sector can likely be traced to concern about the safety and security of cloud based applications. What are these risks? Are these risks surmountable?

Notwithstanding the myriad of complex laws that can conceivably apply to the cloud, the relevant legal risks broadly fall under four distinct headings:

- a) data security;
- b) data export;
- c) continuity of access; and,
- d) privity of contract.

Legal risk: Data security problem

Much of the information held by public sector authorities relates to identifiable living individuals. Such information amounts to “personal data” for the purposes of the Data Protection Acts, 1988-2003. Consequently, such authorities must comply with data protection law whenever that data is being processed. This includes the obligation to put “appropriate security measures” in place to ensure the security of the data. Failure to comply with this obligation is both a regulatory infringement and may expose the data controller to a civil suit for damages. This obligation remains with a data controller even if they

use a cloud provider. In other words, if a data controller moves personal data, for example, about its staff, into cloud based storage, and that cloud is hacked, then the data controller may be liable.

This difficulty has been heightened by the fact that many cloud computing contracts are extremely one sided to the benefit of the cloud provider. Particular concern has arisen over the use of “as-is” clauses, which purport to exempt the cloud provider from any liability whatsoever for any loss or damage caused by its service.

Solution

Concern over the loss of control is arguably one of the biggest obstacles when considering a move into the cloud; however, it is far from insurmountable. From a technical standpoint, it should be noted that a cloud provider, which is dedicated to the safeguarding of data, will often have far more elaborate security and back-ups in place than a government agency for which IT is a subsidiary concern.

However, in practice, the key to mitigating this risk is contract. While one-sided contracts do exist, a government agency considering a move to the cloud should negotiate a fair and balanced contract: one that ensures that the government agency is protected. In particular, the agency should insist that:

- a) the cloud provider has sufficient technical safeguards in place and agrees to comply with data protection law; and
- b) the cloud provider accepts liability for any loss or damages caused to the data.

Ideally, the government agency should also seek to be given a right to audit the facilities of the cloud provider; however, in practice and depending on the provider, this may be difficult to secure.

The effectiveness of clever contracting

in neutralising these concerns is well illustrated by the LA-Google cloud computing agreement. Here, Google's offer of strong contractual warranties, including unlimited damages in the event of data breach, was the decisive factor in convincing the City of Los Angeles to move to Google's cloud based services for virtually all of the City's IT requirements.

Legal risk: Data export problem

One of the, perhaps utopian, ideas underpinning the cloud is the concept that data can flow freely and without complication around the world. The reality is far more complex.

Exporting personal data outside of the European Economic Area (EEA) is a highly complex matter and is governed by the Data Protection Acts. Simply put, in the absence of certain specialised arrangements, personal data can only be exported with the consent of the data subject. In practice, such consent will often not be available.

In addition, public sector bodies must be cognisant of the considerable security risks that flow from moving sensitive government data out of the jurisdiction (and not just outside of the EEA). Cloud providers in the United Kingdom may be required to handover the data they store to the British government under the UK Regulation of Investigatory Powers Act. Similarly, any cloud data stored in the US may be accessed by the US government under the PATRIOT Act. Concern about risks of this nature have led the French government, for example, to instruct its senior civil servants to discontinue the use of their Blackberries, due to the fact their emails would be stored outside of France.

Solution

A government body can export data outside of the EEA in compliance with the Data Protection Acts through the use of standardised contracts called Model Form Agreements. These agreements are published by the European Commission and require that the data importer undertakes to process the data in accordance with European data protection standards. The Commission has recently published revised agreements that are specifically designed to take account of cloud computing. Alternatively, if the data is to be exported to the US, then difficulties may be avoided by ensuring that the data importer is a member of the "Safe Harbor" scheme. Safe Harbor is an arrangement between the EU and the US Department of Commerce under which US companies voluntarily agree to comply with European data protection law.

Where sensitive government data is involved, a twofold risk minimisation

strategy could be adopted.

First, government agencies may choose not to store potentially sensitive information in the cloud. For example, in the US, the Federal Government is encouraging the use of open public clouds for non-sensitive data, while, perhaps unsurprisingly, keeping its most sensitive national security information under tight control.

Second, the government may insist that clouds be located within their own jurisdiction. This approach has been adopted by the Canadian Provinces of British Columbia and Nova Scotia, which have both passed laws to prevent public sector authorities from moving personal information outside of Canada. However, it should also be noted that in British Columbia, it has been proposed that this law be relaxed to allow for non-sensitive public sector information to leave Canada. The motivation behind these proposed reforms is a desire to take full advantage of cross-boarder cloud services.

Legal risk: Continuity of access problem

Public sector bodies are under a variety of retention obligations. Records must be kept available to be meet requests under the Freedom of Information Acts or may have to be stored for posterity under the National Archive Acts. In addition, under the Data Protection Acts, citizens have a right to access data held about them and to order its rectification (if it is incorrect) or deletion (if there are no legal grounds for its processing). While these obligations may stem from a myriad of statutes, they are underpinned by a single key principle: certain data must be stored safely for long periods of time, and must be easily accessed and amended. A particular risk here is the fact that the cloud provider could go out of business.

While these obligations may seem onerous, it worth noting that many private bodies are under similar obligations, particularly with regard to mandatory retention periods under tax, employment and health and safety law.

Solution

A public sector body should be able to ensure compliance with its statutory retention obligations through careful contracting. In particular, it may wish to insist that any data it places into the cloud is properly backed up. In addition, to avoid the possible insolvency risk, a public body should ensure that the contract makes provision to enable the efficient return of any data during the winding-up of a cloud provider. Again, careful review of the terms on offer is key. With the right legal, technical and business continuity arrangements in place, access

to information via the cloud can be more efficient than accessing such information via legal non-cloud based systems.

Legal risk: Privity of contract problem

As noted at the outset, many companies, called "end user service providers" have begun to use the cloud to offer online services to businesses and customers. Such companies may rent the necessary computing power from a third entity, a "cloud provider". However, if the cloud platform itself fails, then the lack of a direct contract between the user and the cloud provider may limit the remedies available.

Solution

There are two ways to overcome this difficulty.

First, the public body can insist that the end user service provider accepts liability for any loss of service, even where it is caused by the cloud platform. A condition like this is unlikely to be accepted without negotiation but an end user service provider may be prepared to accept this liability to win a sufficiently large contract.

Second, the cloud provider may be made a party to the contract between the public body and the end user service provider. This practice is becoming increasingly common as cloud providers often wish to have a direct contract with the end-user, as the public body would be here, to protect themselves, if the end user misuses the facilities provided.

Conclusion

Cloud computing has the potential to deliver immense benefits to both the public service and the nation as a whole. The cloud poses difficulties but these are surmountable through clever contracting. If contracts are the key to the effective adoption of the cloud, then bargaining power in any negotiation becomes all important. Individual government agencies may lack the sort of commercial clout necessary to secure the best possible agreements. To overcome this difficulty, the Irish public service, like its UK and US counterparts, should develop a coherent and standardised cloud strategy. This would allow the State to employ economies of scale to maximise available cost savings, get the best contractual terms possible and deliver an effective stimulus to a nascent Irish industry.

Philip Nolan is a partner and head of commercial in Mason Hayes+Curran. Oisín Tobin is a trainee solicitor with Mason Hayes+Curran. He is a PhD candidate for Trinity College Dublin and is writing his doctoral thesis on the legal implications of cloud computing.