

## Cloud Computing and Data Protection

By Tim Turner

The issue of cloud computing has been getting huge coverage in recent years for a number of reasons – like the new cookie rules, the word ‘cloud’ offers journalists the opportunity to come up with easy punning headings about “storm clouds” or “cloudy outlook”. Moreover, with a myriad of different companies large (Apple, Microsoft, Google) and small offering a variety of cloud products to both organisation and consumers, the horizon is clouded (see what I did there?) with press releases, interviews and advertorials, all designed to persuade people to part with their data. Having sold you the equipment to do the job, the software to process it, cloud providers are now determined to get a slice of the cost of the work you’re actually doing.



So what is cloud computing? This is the easy part – cloud computing is basically an outsourcing project. Instead of storing your data or your software on your network, you pay a company to store them for you. Instead of maintaining a technical infrastructure in order to manipulate, calculate or whatever else you do with your information, you log in through the Internet and do it on the cloud provider’s systems instead. There is no single cloud model, and so underneath the umbrella (I’m at it again), you might go for a wholesale transfer of services, put one part of your organisation onto the cloud, choose one cloud service (i.e. email, like the pilot being carried out by Warwickshire Council), or even just but a cloud back-up. As a computer user, I have everything backed-up twice, and I personally don’t trust some faceless corporation with my precious presentations or my long-gestating novel. But nevertheless, I use Hotmail for all my dealings with Act Now and the people I train for them, and I pay Apple for an iCloud backup of all my iTunes music, meaning that I can access it anywhere and know that I can always get them back.

The perceived advantages of the cloud are many and various – chief among them is the fact that it often works out cheaper to outsource your IT provision to a cloud provider. You’ll need less equipment and less staff to maintain it. Many cloud providers stress the speed with which their systems work, offering further cost savings in terms of efficiency. The fact that data is available via an Internet connection rather than a closed network also offers the possibility of staff working much more flexibly (home working with staff using their own equipment offers yet more savings).

To be fair to the cloud providers, they should also be able to offer all of the software updates, virus protection, firewalls and other technical patches. And of course, as I have already mentioned, the cloud model is built on back-up. Your data will be stored remotely,



and probably disaggregated and spread across a variety of different subcontractors, meaning that if disaster strikes, your eggs are not all in one basket. Indeed, tiny meaningless bits of each one of your eggs will be stored in a wide variety of baskets, and the baskets may move around. And now, let's leave this tortured metaphor in peace.

So that's how it works – what are the Data Protection implications? Here, there are two interesting areas and for the purposes of this article, I'm largely going to ignore one of them. Many big cloud providers are US-based, and there has for some time been an argument between them and the EU about the extent to which the widespread use of cloud services, effectively transferring data and services outside the European Economic Area, is compatible with the European Data Protection Directive, from which our Data Protection Act is derived. This is a debate to keep an eye on, especially as some people believe that the revisions currently contemplated to the Directive are in part designed to bring the US into line with European Data Protection rules. We don't know what the EU is going to propose (and publication of the new proposals has itself been pushed back from January 2012 to February or March).

So we'll keep an eye on that debate, but concentrate for the rest of this article on the practical issues that an organisation needs to take into account when thinking about cloud computing.

### **Fairness**

Perhaps the most important concept in Data Protection is fairness. Although cloud computing is seen entirely as a matter of technology and infrastructure, its introduction nevertheless represents a massive change in how data is used and accessed. Instead of being held by your castle walls (however robust they might be), the data will instead be airborne (albeit protected by encryption wizardry). So can your cloud project go ahead without telling the public? Will your use of their data be fair? And will they go nuts if you tell them? (Yes)

### **Accessibility**

It would be unfair to raise the spectre of an internet-based computer service suddenly becoming unavailable when many in-house networks already suffer 'outages' (the IT industry's euphemism for 'lack of service') without any help from outside. Nevertheless, many of the major cloud providers have suffered such embarrassments (put the phrase 'cloud computing outage' or 'cloud computing breach into your search engine for more) and no cloud provider can guarantee their system is glitch free. It's not inconceivable that a change to the cloud may introduce a more stable network, but this will depend on the quality of your Internet connections as much as it will on the quality of your provider.

### **Security**

Principle 7 says that appropriate organisational and technical measures must be taken to prevent accidental loss or damage to data, and against theft and unauthorised access. Recent history shows a parade of clodhopping security blunders, some of which are linked



closely to a more flexible approach to IT. As well as the inherent loss of control involved in a cloud contract, two other issues need to be considered. Even though it is entirely possible for a cloud provider to offer state-of-the-art technical measures, that will not take care of the new security implications of a flexible, cloud-based way of working. The stories of lost pen-drives and laptops have not dried up even before the widespread adoption of cloud services. The other problem, of course, is that no matter how well funded and established your cloud provider is, your organisation is entirely responsible for any problems that occur – you cannot outsource your legal responsibilities.

### **Location**

The eighth Data Protection principle states that personal data must not be transferred to a country outside the EEA (i.e the EU, Norway, Iceland and Liechtenstein) unless that country has adequate Data Protection laws in place. The US, home of much of the cloud industry does not meet that requirement, although companies which submit to the rigours of the Safe Harbor agreement do. Moreover, the USA has powers under the PATRIOT Act, giving the US government very wide powers of access to any data stored within its borders. This has made the Canadian government very nervous about cloud computing involving US companies, and must be a cause for concern elsewhere.

At the very least, a US cloud provider that is not signed up to Safe Harbor is off-limits for UK customers. Furthermore, the distributed nature of the cloud model, with providers using a variety of storage subcontractors, means that a cloud provider may be unwilling or possibly even unable to tell customers where their data is being stored. Given the necessity to shave off costs in order to offer that Great Cloud Saving, it's unlikely that your data will end up being stored in a nice, stable country like Switzerland.

### **The contract**

In fact, for all the fuss made about cloud computing, in one vital way it isn't any different to any outsourcing contract. What matters is the contract and the demands that you make of the contractor. Inevitably, your cloud provider will be bigger and better funded than you. Anecdotal evidence suggests that some cloud providers make an assumption that you will accept the service as they normally provide it, and questions about where your data will be stored are unwelcome; equally, some providers will tag your data in order to provide a guarantee that it will not be stored outside the EEA.

The crucial thing is that your organisation is responsible for getting the right answers to the vital questions. The problem is that getting those answers is going to be considerably harder than it might be for a normal IT contract.

- Where is your data going to be stored, and who will get access to it?
- What are the security arrangements in terms of firewalls, virus protection, software updates and so on?
- What guarantees do you have for business continuity and back-ups?

- Will your cloud provider compensate you when things go wrong? Will they pay any fines you receive under the Data Protection Act for a breach of Principle 7?

The cloud is clearly the future. Virtually every IT company is betting on it, and the choice to use it is probably 'when', rather than 'if'. What you need to do is decide how you can ensure that you are legally compliant, especially if the storm clouds gather (sorry, couldn't help it).

*Tim Turner is a trainer and consultant on data protection and freedom of information. He runs our online course on Cloud Computing: <http://www.actnow.org.uk/courses/753>*

## ISEB Certificate in Data Protection

An Internationally Recognised Qualification



Act Now is one of the UK's leading providers of the ISEB certificate in Data Protection with a very high pass rate. This course is ideal for those who wish to have their knowledge and expertise recognised through a formal qualification. It is designed in such a way as to allow those with a basic knowledge of DP to benefit and take the exam. The courses run in Birmingham, Belfast, Cardiff, Manchester and London.

For more details: <http://www.actnow.org.uk/content/29>