SHELTER FROM THE STORM

Alasdair Davidson and **Rupert Morris** discuss how to keep you and your data safe when using cloud-computing services

IT HAS BEEN estimated that Amazon's web presence, including its cloud services, accounts for 1 per cent of all North American consumer internet traffic.[1] Added to that, Amazon Web Services, its cloud-computing arm, brought in 5 per cent of the company's total revenue in the first quarter of 2013.[2] This is likely only to increase over the next few years. Big internet companies such as Google, Microsoft and Amazon have ramped up their offering of cloud services in the past 12 months, and the convenience of 24-hour access to documents and data from anywhere in the world is being sold as the next big innovation in business computing.

Much publicity has been given to the benefits of such systems, but what might a business have to sacrifice in return for such convenience? Once your business's and your clients' data has been given up to the cloud, how sure can you be that it is kept securely and that it is still under your control?

If you've ever used a service like Dropbox or Amazon's Simple Storage Service to send or view a document on your tablet, smartphone or Kindle, the chances are that this is now permanently stored on a server in one of the many data centres located in the US or the EU.[3] Can you really be sure that such data will remain confidential to you and your clients, particularly if you or your clients are located, or have interests, offshore? How sure are you that it is secure, not only from cyber-criminals, but also from surveillance by foreign government agencies? Such concerns are by no means far-fetched. They were sufficient, in late 2011, for London-based defence contractor BAE Systems to drop plans to use Microsoft's public cloud-based offering, citing fears that critical defence secrets would end up in the hands of foreign governments.[4]

These concerns are directly relevant to the private client industry and its practitioners as a result of the US *Foreign Account Tax Compliance Act*, the US *Patriot Act* and concerted US and UK government attacks on offshore jurisdictions. It is critical, therefore, that wealth management professionals consider these key factors before heading to any cloud-based solution:

- Control: who has ultimate control and governs access to any data kept for clients in the cloud? Critically, where is it going to be stored?
- Data: what information will be kept in the cloud? Will clients mind that data leaving the jurisdiction in which you or their businesses operate, and being kept elsewhere?
- Value: does the reduced cost of cloud use outweigh the risks for your clients?

1. Estimates by Deepfield Inc. See Craig Labovitz, 'How Big is Amazon's Cloud?', 18 March 2012
2. Netcraft.com, 'Amazon Web Services' growth unrelenting', 20 May 2013
3. www.dropbox.com/help/7; aws.amazon.com/s3
4. 'Defence giant ditches Microsoft's cloud citing Patriot Act fears', Zack Whittaker (ZDNet.com, 7 December 2011)
5. 'Fighting cyber crime and protecting privacy in the cloud', Prof Didier Bigo (EU, October 2012), p14 and p38
6. *Data Protection Act 1998*, ss5(1)(b), 17 and 21
7. Bigo, p33
8. *In re: Directives [redacted text] Pursuant to Section 105b of the Foreign Intelligence Surveillance Act* (US Foreign Intelligence

ALASDAIR DAVIDSON **TEP** IS A PARTNER AND HEAD OF LITIGATION IN GUERNSEY AT BEDELL CRISTIN

RUPERT MORRIS IS AN ADVOCATE AT BEDELL CRISTIN, IN GUERNSEY

These factors can coincide easily. For example, in using the cloud for data storage, how do you address potential breaches of client confidentiality, local data protection laws, and the possibility of exposing clients (and perhaps service providers and their officers) to criminal sanctions and even extradition to the US, the EU or further afield?

Data location and jurisdiction

Jurisdiction and location are often critical factors for clients when choosing a financial services provider, and clients would probably expect any data to be stored in, and only in, their chosen location. As the custodians of confidential and valuable data, service providers need to know where such data is located at all times. However, if a business uses a cloud environment, all data and applications are hosted in the cloud, with data travelling over the internet to one or more externally managed data centres in multiple locations around the world.

Location matters, especially from a legal standpoint; once data is in the cloud, sovereignty over it is surrendered and it is impossible to be sure that the data will reside or remain in any particular location or jurisdiction, or retain its confidentiality. If you do no business with the US, choosing a European-based service provider does not necessarily provide an answer. A recent study from the EU's Directorate-General for Internal Policies[5] revealed that most cloud providers in the EU are reselling services controlled and designed in the US, and their privacy policies state that data will be exported to the US.

In the cloud, the location of the provider's data centres may have consequences for a business. If the cloud that hosts your data has servers in foreign countries, the laws of those countries are likely to be the primary laws that govern any data stored on those servers. Private client businesses must check that their cloud-computing contracts identify where their data centres are located (and potentially even the headquarters of the cloud service provider itself) and match this, wherever possible, to their clients' needs.

Data protection

A clear example of the pitfalls for businesses using cloud computing, particularly in the British Crown Dependencies, can be seen in the UK *Data Protection Act 1998*. Each dependency has its own data protection regime, and one might be forgiven for thinking UK data protection issues might be of little application. However, the UK Act applies not only to UK businesses but also to data controllers (wherever established) using equipment located in the UK to process data. This means a non-UK company using a cloud service provider with servers or data centres in the UK must comply with the UK *Data Protection Act* (such as its provisions on registration), whether or not it does business in the UK, or face (potentially criminal) sanctions.[6]

Similar provisions apply in the data protection laws of the 30 other European Economic Area member states, as well as in other countries. These laws have extensive requirements, restrictions and prohibitions on what can and cannot be done with personal data, and many (including the UK Act) require registration with the jurisdiction's relevant data protection authority. Thus, where a cloud service provider elects to install its servers may have serious consequences for businesses.

National security

Cloud providers are mainly transnational companies and are therefore subject to the conflicts of international public law. Which law they choose to obey is likely to be governed by the penalties applicable in the relevant jurisdiction and, quite possibly, the predominant allegiances of the company's head office management.[7] In principle, access to data by third parties (even governments or their agencies) is restricted without a warrant or court order; in practice it may depend on far more subjective matters.

However, as the Edward Snowden affair has shown, in the past decade some jurisdictions have taken measures to curtail rights to privacy in the names of national security and counter-terrorism.

Much media focus has been on the restrictions brought about under the *Patriot Act*. There has been, until Snowden, little consideration of the implications of the *Foreign Intelligence Surveillance Act Amendments Act 2008* (FISAAA), s1881a of which creates a power of warrantless mass surveillance aimed at the data of non-US persons located outside the US. The FISAAA applies to cloud computing and means it is lawful in the US to conduct purely political surveillance on foreigners' data accessible in US clouds. Data that ends up stored in US data centres is, therefore, potentially liable to such surveillance by federal agencies for the purposes of furthering US foreign affairs, as well as for the more traditional purposes of countering terrorism and money laundering.[8]

The US is not the only data-storage location that might give pause for thought. If, for example, your data is stored in India (a popular location for such services), it will probably be subject to India's *Information Technology Act 2000* (as amended), which allows the monitoring and collection of data traffic by government agencies for public order, security or investigatory reasons.[9] Thus, while a cloud service provider may take advantage of a country's friendly business environment, it may also unwittingly subject its clients' data to the laws and monitoring of countries other than those in which the customer has chosen to operate.

Should you use the cloud at all?

The cloud has the potential to be of great benefit to private client businesses, especially given the international nature of the sector. However, those considering using such tools need to be aware of the pitfalls, including where the data is stored and the foreign laws that may apply. Be sure that the use of such services does not breach client confidentiality or expose clients to jurisdictions where they have chosen not to operate. The safest course is for businesses seeking to use the benefits of cloud computing to set up and operate their own cloud networks. The possible advantages, in the form of reduced costs and enhanced levels of service to clients, can be seized provided careful consideration is given to the contractual terms and the way data is handed over to cloud providers. ■

Surveillance Court of Review no. 08-01), 22 August 2008

9 The Indian *Information Technology Act 2000* (as amended by the *Information Technology Amendment Act 2008*), s69