Storm cloud on the horizon - How safe is your information and how safe are you?

2012 has been the year of the cloud. It is estimated that Amazon’s cloud services alone now account for at least 1% of all internet consumer traffic and that this is likely to only increase over the next few years. The big internet companies, in particular Google, Microsoft and Amazon, have ramped up their offering of cloud services over the past 12 months, selling the convenience of 24/7 access to your documents and data from anywhere in the world as the next big innovation in business computing.

However, whilst a great deal of publicity has been given to the benefits of such systems, there has been comparatively little coverage of what a business might have to sacrifice in return for such convenience. Once your business’ and your clients’ data have been given up to the cloud, how sure can you be that this is kept securely and still under your control?

If you have ever used Dropbox or Amazon to view a document on your iPad or Kindle, then this is now permanently stored on a server in one of Amazon’s many data centres somewhere in the United States or the European Union. Can you really be sure that such data will remain confidential to you and your clients? 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 to drop plans to use Microsoft’s public cloud-based offering, citing fears that critical defence secrets would ultimately end up in foreign government hands.

In the era of FATCA, the Patriot Act and concerted US and UK government attacks on supposedly "harmful" offshore jurisdictions, these concerns are directly relevant to the Channel Islands’ financial services industries.

The key message is therefore that before using a cloud, it is critical that local businesses consider what information and data they might be giving up and whether they mind such information leaving the Islands to be stored elsewhere. Not to do so might potentially breach client confidentiality; local data protection laws; as well as possibly exposing clients (and even local service providers and their officers themselves) to potentially unknown criminal sanctions and even extradition to the US, the EU or further afield.

Data location and jurisdiction

In the offshore world, jurisdiction and location are often critical factors for clients when choosing a financial services provider and clients would probably expect any data also to be stored in, and only in, their chosen location.

Location matters, especially from a legal standpoint - once data is transferred to a cloud sovereignty over it is almost inevitably
In a cloud environment the location of the provider's equipment and data centres may have significant consequences for a business - if the cloud that hosts your data has servers in foreign countries then the laws of those countries will likely be the primary laws that govern any data of yours which is stored on those servers.

In a cloud environment the location of the provider's equipment and data centres may have significant consequences for a business - if the cloud that hosts your data has servers in foreign countries then the laws of those countries will likely be the primary laws that govern any data of yours which is stored on those servers. As such it is critical that local businesses check that their cloud computing contracts identify the geographic regions in which their data centres are located (and potentially even the headquarters of the cloud service provider itself) and limit these wherever possible according to their and their clients' needs.

Data protection
A clear example of the potential pitfalls for local businesses when using clouds can be seen in the UK Data Protection Act 1998. Of course, Guernsey and Jersey have their own Data Protection Laws and one might be forgiven for thinking that UK data protection issues might be of little or no consequence here. However, when one considers that 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, then the concern becomes very real. This means that a local 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.

Similar provisions also apply in the data protection laws of the 30 other EEA 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 your cloud service provider elects to install its servers may have serious consequences for your business.

National security and the fight against terrorism
Cloud providers are mainly transnational companies and are therefore subject to the conflicts of international public law. Which law they choose to obey will likely be governed by the penalties applicable in the relevant jurisdiction and, quite possibly, the predominant allegiances of the company's head office management. 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 upon far more subjective matters.

However some jurisdictions have taken measures over the last decade to curtail such rights to privacy in the names of national security and counter-terrorism.

Much of the media focus has been on the restrictions to freedoms brought about under the US Patriot Act. There has been, however, virtually no consideration or discussion of the implications of the Foreign Intelligence Surveillance Amendment Act 2008 (“FISAA”), s.1881a of which creates a power of warrantless mass-surveillance specifically targeted at the data of non-US persons located outside of the US. The FISAA applies to cloud computing and means that it is lawful in the US to conduct purely political surveillance on foreigners' data accessible in US clouds. This means that any data which ends up stored in US data centres is potentially liable to such surveillance for the purposes of furthering US foreign affairs, as well as for the more traditional purposes of countering terrorism and money laundering.

It is not just the storage of data in the US which can give rise to such concerns. If your data is stored on a server in India, for example, (a very popular location for such services) it will likely 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. Thus, whilst 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 where the customer has chosen to operate.
Extradition
Given the potential scope for surveillance of data stored in the US and elsewhere, there is also, inevitably, the risk of governments taking enforcement proceedings against foreign nationals, including criminal proceedings for which extradition may be sought. The very public attempt by the US to extradite Kim DotCom from New Zealand for breach of copyright laws is one such example, but there have also been instances of US attempts to extradite UK citizens on tax-fraud charges, such as with the London-based hoteliers, Stanley and Beatrice Tollman.

Whilst there have so far been no attempts by any foreign government to extradite Guernsey residents, the same cannot be said for Jersey. In the first extradition application under the Extradition (Jersey) Law 2004, in November 2010 a Jersey resident individual, Philip de Figueiredo, was successfully extradited to Australia to face charges of tax fraud.

Jersey legislation provides for extradition where a valid request is made by a foreign territory in relation to a person accused of committing an offence in that territory (referred to as a ‘designated territory’). The Jersey law distinguishes between designated territories of the first and second category. The first category includes, for example, many European countries, the US and Australia, whilst the second category includes some African, Asian and Latin American countries amongst others. If a request for extradition is made from a second category designated territory, there are more stringent requirements on extradition, and the Jersey courts will need to consider whether there is sufficient evidence for that person to stand trial once extradited. There are a wide range of offences for which a person can be extradited from Jersey.

Unlike in Jersey, extradition in Guernsey remains governed by the UK Extradition Act 1989, which still requires a requesting country to provide evidence to establish a prima facie case (i.e. one which would be sufficient to convict if no defence was offered). However there has been an ongoing review of the position by the Guernsey authorities, since 2007, to bring Guernsey (like Jersey) more in line with the, significantly less onerous, US-UK Extradition Treaty 2003 (requiring as it does the US to only provide information as to any offence as opposed to evidence).

Should Guernsey choose to follow Jersey's lead then non-US companies and their officers based in Guernsey will need to be aware of the increased risk of extradition to the US, particularly given the limited defences one can put under the proposed regime and the potentially wide range of offences for which extradition may be sought.

Should one use clouds at all?
Clouds clearly have the potential to be of great benefit to offshore businesses, especially given the international nature of much of the financial services work undertaken here. However local businesses considering using such tools need to be sure of the precise locations where their data is stored and the various foreign laws which may apply to such data and, if necessary, take appropriate advice. They will need to be sure that the use of such services does not breach client confidentiality nor unnecessarily expose clients to jurisdictions in which they have opted not to operate. The safest course, of course, is for businesses seeking to use the benefits of cloud computing to set up and operate their own cloud networks. However, if this is not an option then local companies should think very carefully before sending information to public cloud providers and should seek to carefully negotiate any contracts for such services to ensure that they retain some measure of control over their data.

"The very public attempt by the US to extradite Kim DotCom from New Zealand for breach of copyright laws is one such example, but there have also been instances of US attempts to extradite UK citizens on tax-fraud charges, such as with the London-based hoteliers, Stanley and Beatrice Tollman."
For further information, please contact:

**Jersey**

David Cadin  
Partner  
T +44 (0)1534 814701  
E david.cadin@bedellcristin.com

**Guernsey**

Alasdair Davidson  
Partner  
T +44 (0)1481 812819  
E alasdair.davidson@bedellcristin.com  
Rupert Morris  
Advocate  
T +44 (0)1481 812851  
E rupert.morris@bedellcristin.com