For some time I've watched as New Zealand businesses have been seduced by the so called advantages of Cloud Computing.

In a manner similar to drug pushers, they dole out free "hits", they eschew free services that entice business owners to send their IT provisioning to places unknown overseas. The glamour of the websites, extolling these services, appears to induce a feeling of security, all the while containing many a fish hook.

The first issue is Privacy.

In New Zealand we have a comprehensive Privacy Act , to which our local businesses must comply. They cannot transfer that responsibility to overseas cloud providers.

So what are these Privacy Issues?

One of the 12 Principles of the privacy Act 1993 states:
Principle 5: Storage and security of personal information

An agency holding personal information must ensure that:

- there are reasonable safeguards against loss, misuse or disclosure; and
- if it is necessary to give information to another person, such as someone working on contract, everything reasonable is done to prevent unauthorised use or unauthorised disclosure of the information.

Ref: http://privacy.org.nz/information-privacy-principles

This Principle is quite an onerous obligation. What this means is that if you (the agency) are responsible (a) for safeguarding any data on individuals collected, (b) for any misuse of that data, (c) if it is accidently disclosed.

Further, if the data is given to another party, you must do everything reasonable to prevent unauthorised use.

Now this latter point if of significance. It is not enough to tell the other party of the regulations, or even have them sign an agreement that includes the provisions. It is necessary that you "do something".

Signing a Contract with relevant clauses is a very minimum of what can be done. It is only a baseline. And relying on the Cloud Providers Standard Terms & Conditions is not a good position, particularly if you need to defend a potential breach.

And even if you have taken the time to complete the detailed (and sometimes costly) steps to cover yourself, can you be certain that you have "done everything reasonably within your power". You are right to question whether filling in a few details online and clicking “I agree” to

the Cloud Provider's Standard Terms * Conditions will be sufficient.

Also few consumers of Cloud Computing services actually carry out independent audits, to ensure compliance with any contractual elements related to Privacy.

Another Principle in the Privacy Act can also raise an issue.

Principle 3: Collection of information

When an agency collects personal information directly from the individual concerned, it must take reasonable steps to ensure the individual is aware of:

- the fact that the information is being collected;
- the purpose;
- the intended recipients;
- the names and addresses of who is collecting the information and who will hold it;
- any specific law governing provision of the information and whether provision is voluntary or mandatory;
- the consequences if all or any part of the requested information is not provided; and
- the individual's rights of access to and correction of personal information.

Ref: http://privacy.org.nz/information-privacy-principles

As a collector of information from individuals, you are required to take "reasonable steps" to make each individual aware of who is holding the information.

If you using a Cloud Provider, particularly overseas, then that must include them. If not, then you are more than likely in breach of this principle.

The second issue is Security

The analyst firm Gartner have stated that Cloud Computing is fraught with security risks.

Ref: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853

Gartner identify seven major risk areas that should be addressed with any Cloud Provider:

1. Privileged user access. Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs. Get as much information as you can about the people who manage your data. "Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access," Gartner says.

2. Regulatory compliance. Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers who refuse to undergo this scrutiny are "signaling that customers can only use them for the most trivial functions," according to Gartner.

3. Data location. When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers, Gartner advises.

4. Data segregation. Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. "Find out what is done to segregate data at rest," Gartner advises. The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists. "Encryption accidents can make data totally unusable, and even normal encryption can complicate availability," Gartner says.

5. Recovery. Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster. "Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure," Gartner says. Ask your provider if it has "the ability to do a complete restoration, and how long it will take."

6. Investigative support. Investigating inappropriate or illegal activity may be impossible in cloud computing, Gartner warns. "Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then your only safe assumption is that investigation and discovery requests will be impossible."

7. Long-term viability. Ideally, your cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But you must be sure your data will remain available even after such an event. "Ask potential providers how you would get your data back and if it

would be in a format that you could import into a replacement application," Gartner says.

In the Real World

In the reality of day to day operations of any IT service, you must ask yourself, "**do you own your data?** ".

Just getting access to a copy of it is not enough in the writer's opinion to define ownership. **To fully own data you must control it, be able to determine it's destiny, location, and control the parameters around it's spread**
.

If you do not control the destiny of your data and systems, then you have given that ownership to someone else. And in one specific case, placing that data in the hands of a Search Engine provider whose very business is analysing data, is somewhat akin to putting your money in a bank run by Ronald Biggs .

Over the last few years there have been a number of incidents at large Data Centres, that have literally had the capacity to put businesses, out of business. The one that immediately comes to mind is the explosion and fire at the Houston data centre operated by The Planet in 2008 . This affected over 9,000 customers. Due to the nature of the problem, the local fire department did not allow them to operate backup generators. Some customers were not able to access their system for up to 10 days.

Other providers may have systems that extend across multiple Data Centres, or have learned from the example above (well publicised and analysed by those in the Data centre fraternity I'm sure)

Conclusion

So this is very much a case of buyer be aware. Be aware of the downsides, as they may relate to you and your busienss. Be aware that if you hold sensitive information - and that may just be a lit of your customers, and their personal contact details - you are responsible under the terms of the New Zealand privacy Act 1993.

The Privacy Commissioner is currently reviewing this whole issue as it pertains to Cloud Computing. You may wish to read this article from a talk to the NZ Computer Society in Wellington in March 2011.