KEEP YOUR HEAD IN THE CLOUDS

Category: Privacy Law, Infosec, and POPIA,Technology Law
written by Yashoda Rajoo | June 26, 2018

The world is running out of space. Parks are becoming buildings, highways are ploughing through farmland and your Blackberry that could store hundreds of photos has turned into your iPhone that can store thousands. Who needs a memory card or USB in the era of *dunt dunt dunt…* **THE CLOUD**.

We all know of cloud storage, and we've all heard of cloud hacks, but how dangerous is the cloud really? Is our data at risk? This article looks at how the three main cloud storage facilities deal with our data in transit (data that is moving from one location to another) and our data at rest (data that is stored in a specific location). Data is exposed to risks both in transit and at rest and needs to be protected at all times.

Dropbox

In transit, data is protected using Secure Sockets Layer (SSL). This is security technology which creates an encrypted link between a server and a client. At rest, data is protected using AES-256 – bit encryption. This is a very long key, which, to date, has not been cracked. Dropbox holds the keys to this encryption. Dropbox is transparent, and makes it clear that certain information is shared with employees and trusted third parties, but undertakes not to sell your information to advertisers or other third parties.

iCloud

While iCloud uses SSL to encrypt data in transit, it uses a "minimum of 128 – bit AES encryption" which, it can be argued, is half as secure because it is half as long as the 256 – bit AES. iCloud protects your data with a key derived from information that is unique to your device. They aver in their security overview that they use end to end encryption, and assure "No one else can access or read this data."

Google Drive

Like iCloud, Google Drive uses SSL to encrypt data in transit. Data is stored at rest using 128 – bit AES. The main issue with Google Drive is that the correct login information grants access to all Google accounts. While this creates convenience, it also places greater responsibility on the user to protect their login details.

The reality is that “the Cloud” is relatively reliable. The service providers endeavour to keep your data safe, as well as constantly accessible. They have the money and resources to protect your data far better than if you try to protect it on your own. With the GDPR now in full force and effect, their incentive to protect your data is greater than ever. So, while storing data in the Cloud may be a risk, it definitely is a risk worth taking.