HOW TO AVOID YOUR BUSINESS BEING SPIED ON BY THE US (ANY OTHER) GOVERNMENT

Category: Commercial Law,Privacy Law, Infosec, and POPIA,Technology Law
written by Lucien Pierce | June 30, 2013

A 29-year old called Edward Snowdon last week blew the whistle on the US Government's snooping program. What conspiracy theorists have been scaremongering about and what Jason Bourne fantasised about is chillingly true: the US Government has access to much of the information housed on servers in the US.

The US Government has been scrambling to contain the fall-out of Snowdon's revelations that its National Security Agency (NSA) uses a monitoring program called PRISM to collect the information of millions of people. According to the UK's Guardian newspaper "identifying information" or metadata of the calls of millions of people on Verizon's network in the US have been recorded.

To make matters worse, further revelations claim that the NSA is able to tap into the servers of Yahoo, Google, Facebook, YouTube, Skype, and Apple (these companies have denied these claims). The NSA can obtain copies of search history, the content of "*email, video and voice chat, videos, photos, voice-over-IP (Skype, for example) chats, file transfers, social networking details, and more*".

Whilst South African companies might try to console themselves by thinking that only the information of individuals and businesses in the US may have been monitored, they would be wrong. It's quite likely that if your business makes use of, for example, Google for Business or one of the cloud based services hosted by AOL or Microsoft in the US, your confidential information is capable of being accessed by agencies such as the NSA. In our case as a law firm, even more worryingly, if we backed-up our confidential information to the cloud in a less than secure manner, the US Government could possibly try to get its hands on our clients' data.

The monitoring of confidential information is not unique to the US and neither is it new. Western governments used monitoring programs such as Carnivore and Echelon in the past, also for purposes of monitoring communications and accessing information. The South African government is also empowered to monitor and access the communications and information of businesses and individuals within South Africa. Their power comes from a number of pieces of legislation, the best known being the Regulation of Interception of Communications and Provision of Communication-Related Information Act ("**RICA**").

RICA permits law enforcement agencies to intercept and require internet service providers and telecommunications companies to provide them with the communications and communication-related information of their customers. This information can however only be requested once a judge has: heard an application from a law enforcement officer; considered the validity of the application; and issued an order directing a telecommunications company or internet service provider to deliver the required information.

RICA is therefore very similar to monitoring and interception laws in the US The consolation for South Africans being that unlike in the US, where the NSA effectively has a very wide and all-encompassing interception order, South African orders authorising interception and monitoring are very specific and limited to a maximum of three months at a time.

So what does a South African company do – one which wants to protect its own data and which has a

legal duty (like us lawyers do) to protect its clients' data? Think about your attorney's office, your hospital, your bank – are they hosting their information in the cloud and if so are they sure of its integrity? As a medium-sized business specialising in information security, we have looked extensively at what we – and our clients – can and should do to protect our information. The cloud is great because it's more reliable than the physical storage we're using at the moment; it's accessible from wherever we may be; and with data prices falling, it's not that expensive.

So, here's what we view as the best of both worlds: the convenience of the cloud PLUS (almost) bullet-proof security.

Firstly, make sure that your cloud service is based in a jurisdiction which has strong information security laws. Our view is that jurisdictions like the EU and South Africa (once the Protection of Personal Information Act or POPI is passed) are relatively safe jurisdictions from an information protection perspective. The EU takes a very dim view of the US Government's access to private information. It takes data security a LOT more seriously that the US and has the legal system to defend your data from access by US snoopers.

Secondly, check your cloud service's terms and conditions. Many cloud service providers have servers in different locations across the globe. Check and confirm where your cloud service's servers are. If they also have servers in the US, check whether you have the choice of choosing a location which is within an information security respecting jurisdiction and not the US. You should also ensure that the cloud service's terms confirm that your data will not be hosted in or transferred to any other jurisdiction other than the one you have chosen. You should also check the confidentiality undertakings that your cloud service makes. An important term would be for them to let you know when they have been served with an order directing them to hand over your information (not so helpful if the order prevents them from doing so, but nice to have just in case the order misses this).

Thirdly, don't be fooled by promises that your information will be encrypted when it is received and hosted on the cloud service's servers. Remember: if the service provider is able to encrypt your information, it also has the ability to use a device or password (sometimes referred to as a decryption key) to unencrypt the same information. The interception legislation in most jurisdictions obliges telecommunications companies and internet service providers, at the risk of very big fines, to decrypt your information or hand over the decryption key. You therefore don't really want them to have this option.

Fourthly, encrypt your information before it is uploaded to your cloud service's servers. There are a number of cloud services which offer excellent software allowing you to encrypt your information in such a way that only you have the decryption key or password. This way, even if the cloud service receives an interception order directing it to hand over your information, it will be able to do so in the knowledge that the information will be difficult if not impossible to be decrypted. Whichever agency obtained the interception order would then have to come to you for the decryption key, giving you time to get legal advice on how best to respond to them without breaking the law.

These simple steps will ensure that you, your clients and customers can have confidence in the integrity of your information and that, whether it be the US or any other government, snoopers will find it very difficult if not impossible to look through your most private information.