Submission No 80

Inquiry into potential reforms of National Security Legislation

Organisation: Kim Riley

Inquiry into potential reforms of National Security Legislation

Cybercrime. Provisions

Without having a clearly defining policy on issues such as processing of business and private transactional data in The Cloud regardless of its location within our Borders or outside.
We are now in an age of increasing use of IN Memory computing hardware and associated software. This provides a revolution in Business analytics and other uses of this technology are endless.
I think it is reasonable to assume that Criminal activities that were easily traceable have now another level of Cover. That will have the potential to affect our National as well as Private Security. It is the dawn of a new age is some ways.

So across all sectors, the commercial push is to drive costs and increasingly to leverage off others investment to transform normal business processes that were done in House. It is now the realm of providers of data transformational services in and outside of our borders.

So this effects the way we use computers, in house business IT systems / platforms that were local and discrete in there setup and operation. These systems are now no longer the pathway that businesses as well as governments are taking!

I work using the ERP product SAP. [From SAP AG], They are the market leader in ERP systems, SAP AG are like other Business application suppliers are moving to develop hosted products. Where the data may originate in within our borders but the transformation of that raw data into financial business outcome is done off shore.

I will use them for my argument, their Technology HANNA In Memory computing is a tool to quickly deeply analyse links, profiles and trends. This potentially includes tracking an individual by the outcomes of their transactions, is something that is now easily achievable.

I expect there are enough Master data identifying characteristics to do this on a commercial scale. It would be possible as the more data goes into the Cloud [regardless of the clouds location, within or not within borders] for Businesses / countries or groups to take commercial and strategic decisions that could destabilize parts of our economy.
SAP HANNA is just one of these Tools available.

This may sound futuristic, but as we not planned for this, with Policies and legalisation, these developments are not in place to prevent this. So it is easy to see the potential effects of this happening.

Until now we have been able to ignore the security aspects of little bit of data / individual items going off shore for processing. Our national thinking is that the commercial imperative out weights any risk. But we failed to realise with these technology advances that these little bits all together, do pose a much larger risk.

As I previously said: This new world is no longer traditionally within Australian borders but In a Place where the only link to Australian Laws is the raw data point of collection.
We need Laws that strengthen the right to privacy. The potential spin off this is a Social one, it is local Investment and increase in confidence, sadly the world needs these too....

***Data is now transformed and stored in the Cloud,**. Not only will technology impact on my personal privacy but the individual businesses and the national security too. These are fair Game for **Anyone**, **anywhere outside of Australia can legally access and or misuse Australian citizen data, because it been sent to an inappropriate place.**

"No amount of holding Australian institutions, responsible" Will make our / my data any more secure off shore. It's fundamentally not protected.

Equipping Australia against emerging and evolving threats paper:

It appears that this paper ignores the threat I have outlined. It looks at life as it was before.
It also looks at the mode of moving information.

It is time to move forward on amendments to National Security Legislation.
As .the information intercepted for national security purposes argument is based on the flow of information within Australia. But If the data is packaged and sent offshore for processing, There is little ASIO can do there to stop cyber crime of Identity / other data trafficking and the subsequent fraud.
As any breach of Privacy can have already happened beyond our Borders long before Australians or ASIO are made aware of this. '

Offshore this is where the Cloud is, by my definition it's a moving linked entity for which data can be stored and transformed.
Currently even locally Hosted Clouds have no guarantees, as we have **no Policy** and subsequent laws and method of enforcement that stop the switch to another hosting location.

I make this statement because I can't see any legal methods of detecting / intercepting changes in the location of data being held.

As it is now possible to Host on the cloud almost for free in China! Or in India! It's a business choice as to which service at the time is the best risk! This choice is one that is managed for us by a NON Australian linked provider

Regards
Kim Riley