Comment on the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

1.0 INTRODUCTION

These comments are to provide additional insight on the workability and usefulness of this Act. Firstly, we review the technical scene upon which this Act may have effect, and then I go into individual technical areas.

My final conclusion is that whilst this Act may have some limited use in Australia, its effect will be very limited, as existing knowledge, technology and internationalization will negate its intent with relative ease. Are these changes a worthwhile addition?

1.1 SETTING THE SCENE

Before commenting on the Act I would firstly like to paint an updated picture of the technologies that are, or will be, available in the near future.

All organisations are required to keep the information they care for private and secure to stop inappropriate access. This is especially true regarding Government and financial information.

Over the years Information Technology (IT) manufacturers have responded to this need by, in part, implementing secure encryption as an integral part of the hardware and communications they provide. At this point the data written and retrieved from/to longer term data storage is securely encrypted, even data used by the processors on computer boards can be treated in this manner as data is written to the dynamic fast memory. Similarly, communication links will secure data as it is transmitted.

Satellites have already been launched and hundreds will follow that will provide instantaneous communications between themselves or any place on Earth - just from something like your mobile phone! No base station is required within the country where the satellite's user resides. Costs will be very competitive with current Earthbound services.

The methodology (and software) of much of the encryption technology is publicly available and can be compiled and installed by a schoolboy on nearly any platform you can think of. In addition, whilst we have international standards on encryption, there are others that can be used that are almost (or more) as effective, and the algorithms for these are easily available and can be implemented similarly.

Much of the World's trade and Government and financial dealings relies on encryption technology for its successful use. Without this and similar technology the complex web of legal and financial details will become insecure and World trading activity will slowly grind to a halt, or at least to the pace before encryption. The issues identified by the UK's Brexit negotiations identify just how often goods are traded crosses international boundaries.

2.0 LIKELY IMPACT OF LEGISLATION ON AUSTRALIA'S SECURITY

Whilst I would agree with the Act's intention; existing and advancing technology may have enabled its enforcement impractical.

The first issue is one of this legislation's scope. It can only be applied to organisations or persons that have some legal basis in Australia. Given the internationalisation of communications, and the integration of superior security into everyday devices, it would appear that much of future information transfer function could be beyond the ability of this Act to control. Information will be stored with and flow through extra-territorial entities.

A side-effect of the Acts enforcement would to restrict the technologies that are imported to be used in Australia. Given that much of the electronics is today mass-produced, over a few years many Australian organisation would be forced to use a dwindling supply of expensive, outdated and insecure technologies. We may find that branches of international companies may not be able to continue business in Australia.

3.0 ACCESS TO DEVICES

Various parts of the act describe access to Devices. Devices are getting smaller and smaller - a mobile phone now fits into a watch. The ability to control the ingress of devices with hardware that implements hardware-based encryption will be extremely limited, and overseas travellers will have easy access to a device, perhaps on their wrist, that will be difficult to detect and monitor under the Act.

3.1 Application of The Act

On the assumption that the holder of the information is unwilling to reveal its contents the Act's basis is its assumption that some third party has the means to access the information or at least has installed some feature that enables the information to be revealed. Without the ability to reveal the data I am not sure of the success of any legal action.

Let us assume that the owner is unwilling to reveal the data! Whilst it is probably possible that some form of revealing technology could be installed in common devices, anyone could easily bypass these eavesdropping capabilities.

4.0 CONCEALMENT

I have met schoolchildren whose hobby it is to construct small computers that can implement security features.

Such abilities rely on a few Principles

Firstly, the availability of Publicly and Easily Available Source Code for both a PC or Mobile Phone's Operation and Its Applications. Much of this code is already used in the mobile phones we purchase.

- Similarly, the availability of the code to encrypt and decrypt data to any level of encryption you wish.

- The ability to create and install your own security software applications that feasibility could bypass any snooping features installed.
- Again, as above, the availability of code to operate your PC or almost any other device you can think of.
- Further, the availability of standard circuit boards where the user can build a suitable system from the ground-up, and with a small amount of knowledge.
- The commoditization of electronic components so that many can be bought off-the-shelf with ease. Control of these off-the-shelf components would prove an almost impossible task as they are used in so many differing areas and would be difficulty to detect.

If we take a standard off-the shelf mobile phone as an example it would be possible to create your own application (App) that would bypass any snooping features and ensure your data is protected.

A further issue arises over a snooping capability. Much of the Worlds commerce relies on the security features in encryption technology. The minute this is effectively endangered nearly every feature that requires storage of data (money and trade) is at risk. Who would do business with Australia under these terms? Nobody!

The real risk from implementing this Act comes from human aspects. Humans are the weakest link in the security chain, and once a single link is weakened; we are likely to find that the whole chain fails.

5.0 THE MULTI-NATIONALISATION OF INDUSTRY AND TRADE

Just as a personal example. I was a member of an Australian small community group with about 1,500 members.

Members' records were within a computer system, but for historical reasons the data for these records was stored in Romania.

This small example illustrates the difficulty that many corporations have in applying a Counties laws to their data holdings. Can you apply one or both countries laws in my own example?

With a larger corporation the data may be spread across several countries or borders depending on the best and most secure place of storage. Storing in one country could represent a greater risk to the security of the data if something calamitous occurred.

Organisations like the Government can contractually insist that a service provider maintain its data within a county's boundary but it is not clear to me, given the way that these large providers work, that you could prove how the data is stored or even that the data does not pass through other countries on the way to its destination. Once your data crosses the responsible corporation's boundary, even they may not know how it arrives at its proper destination!

The above again reinforces the need to ensure that data is encrypted as it is stored or transmitted.

6.0 ISSUES RELATYING TO "THE CLOUD"

Many of us use this every day; in person or within a larger grouping. Your personal data is kept stored on a server somewhere around the World. You do not need a copy on you own device! If you wish, you can encrypt the data you wish to store. You can even share the data with others.

Contrary to much popular TV it is possible to remove traces of a Cloud Stored (or any) document from your own device. If one was really worried about security, today's devices are relatively cheap and could be destroyed and a new one purchased. The issue being that it is most probably that the data is no longer under the jurisdiction of Australian Law, being stored, perhaps in bits and pieces, somewhere else in the World.

7.0 MONITORING OF INTERNAL COMMUNICATIONS

Much has been made of the risks of overseas communication suppliers' products being used for Australian Internal Communications. None are without their risks, even those products from "friendly" nations. They all need some inspection and certification!

Add to this the long existent capability of satellites to monitor such signals as mobile phone and microwave links. The only way to secure data transfer is to securely encrypt the data.

For us to deliberately reduce our level of overall security would make external intelligence agencies think again before sharing their information with Australia.

8.0 CONCLUSION

Whilst I have not addressed particular areas of this legislation (and I am assured that the intent is accurately written into the Act's changes as it applies to Australian bodies). I reiterate that in today's World I have little confidence that you could detect or stop an encryption secured user of moderate skills.

I am convinced that given sufficient computing power some of the more secure encryption methodologies are able to be broken by the Intelligence Services, but this requires considerable computing power, and will take time. Perhaps precious time!

Since some of WW2's codes have never been broken I am confident that brute force whilst of value, will not solve all problems.

Quantum Computing may help but this could be some way-off.

As with the outright banning of 5G Huawei, the changes to this Act's philosophy seem to be driven by an uninformed, uncritical or unlistening group of policymakers.

9.0 SECURITY IN THE MODERN WORLD

Perhaps the challenge is that Governments are stilling thinking about solving problems from a regional/country perspective. The World has moved on and Governments are less and less able to control these areas as in the past. This style of Act risks completely isolating the implementor's societies. To do this could be an economic disaster and be of minimal value.

New techniques need to be found, and these techniques may not rely on technology but on historically effective intelligence methodologies.