benchtv
a benchmark production

Précis Paper

Proposed Encryption Legislation in Australia

A discussion of the proposed encryption legislation in Australia with reference to the existing encryption legislation in other jurisdictions.

Discussion Includes

- What is encryption?
- Encryption legislation in other jurisdictions
- Criticisms of the United Kingdom and New Zealand regimes
- Other potential concerns with the proposed legislation
- Preparation by technology companies

Précis Paper

Proposed Encryption Legislation in Australia

In this edition of BenchTV, Angela Flannery (Partner at Holding Redlich, Sydney) and Karen Lee (Principal at Legal Know-How, Sydney) discuss the proposed encryption legislation in Australia and the existing legislation which deals with encryption in both the United Kingdom and New Zealand.

What is encryption?

1. When people discuss encryption, one of the most commonly given examples is messaging applications like WhatsApp. In messaging services such as WhatsApp, when you send a message, that message is encrypted using a public key supplied by the messaging service. The encrypted message is sent to the recipient. On the phone of the recipient, there is a private key that decrypts the message so the recipient will see the message as it was originally intended. Once the message leaves the sender's phone, it is immediately encrypted and it is not possible to decrypt it unless you have the decryption key, and the only place that key exists is in the recipient's phone.

2. Apart from services like WhatsApp, to take another encryption example, you can also download software that is freely available on the internet to encrypt a message yourself, and then send it through normal communication systems, for example via email.

3. There are different ways that encryption keys can work, and technologies continue to advance with different types of encryption. The concern of the government and why this has become more of an issue in recent times is because of the prevalence of messaging systems like WhatsApp and the increasing use of the encryption services that are available. There is perception on the part of governments which is supported by statistics that encryption may be aiding criminal activity such as terrorists, organized crime and paedophile rings.

4. Law enforcement agencies believe they are being negatively impacted by the use of encryption. Encryption means that law enforcement agencies are having difficulty in determining whether offences are being planned and, how to stop these offences, and more difficulty in prosecuting criminals as they cannot access the encrypted messages.

5. Due to this, the former Attorney-General and the Prime Minister announced that the government would pass encryption legislation, stating that it would be introduced into parliament during 2017. Under that legislation, a broad range of telecommunications and technology companies will be obliged to provide assistance in decrypting messages where that is required by law enforcement agencies.

6. Currently in Australia we have a broad range of legislation that allows for interception and access to communications. The primary legislation is the *Telecommunications (Interception and Access) Act 1979* (Cth). This Act was first put in place in 1979, though it has been significantly amended since then. There are also other provisions in the *Telecommunications Act 1997* (Cth) and the Crimes Acts at both state and federal levels that may be used to intercept and access communications.

7. Under the TIA Act, there is a number of strictly limited number of law enforcement agencies who are able to obtain interception warrants for accessing communications while they are occurring. These warrants are obtainable only in relation to investigation of a fairly limited class of serious criminal offences which have penalties of at least seven years imprisonment.

8. There is another category of warrant which allows a broader category of law enforcement agencies to obtain warrants to allow them to access communications data. This type of warrants can be obtained for a broader range of breaches of law, including breaches that have penalties of three years or more in prison.

9. There is also an authorisation regime which allows an even broader range of law enforcement agencies to authorise telecommunications companies to provide access to telecommunications data. This allows access to data about a communication, for example, to see who called who, when, etc. but it does not allow access to the actual content of the communications.

10. Looking at another example, under section 313 of the *Telecommunications Act 1997* (Cth), carriers and carriage service providers are required to, amongst other things, provide state, territory and Commonwealth authorities with such help as is reasonably necessary for enforcing criminal and certain other laws. There are other laws that allow law enforcement agencies to access communications, which we don't have time to cover here.

11. The government's view is that, notwithstanding the range of regulation that already exists to allow law enforcement agencies to access communications, a broader range of companies need to be subject to regulation and also that specific decryption obligations need to be imposed.

12. At around the same time the encryption legislation proposal was announced, the government also announced the establishment of a new Home Affairs Ministry. Peter Dutton was appointed as the first Home Affairs Minister at the beginning of 2017 and that ministry is taking quite a bit of responsibility in terms of national security from the Attorney-General. A new Attorney-General was also appointed towards the end of 2017. Those political changes, as well as the fact that the government said it would privately consult with a number of

technology companies before introducing the legislation, has caused delays to the originally announced timing for the release of the legislation..

13. The former Attorney-General said in early December of 2017 that there is an advanced draft of the legislation available and that should be introduced to parliament in the first quarter of 2018.

Encryption legislation in other jurisdictions

14. The government has said that it is going to base Australia's encryption legislation on the model currently in place in the United Kingdom. The *Investigatory Powers Act 2016* (UK) covers a broad range of issues. This Act is the framework for security and intelligence agencies, law enforcement and so on, to access communications and communications data.

15. The key encryption related power given to government under the UK legislation is the power for the UK Secretary of State to issue what are called technical capability notices to telecommunications operators. The Act requires the Secretary of State to take into account things like cost before it issues a notice. Those notices requires the operator to take action that will allow it to provide assistance to law enforcement when a warrant is obtained to access communications. A notice is not a warrant, it is a requirement to ensure that technical capability is in place with that telecommunications operator so that it can provide assistance should it be necessary.

16. The technical capability notice provisions of the UK legislation have not yet taken effect because it is necessary to put in place some supporting regulations and codes. The *Investigatory Powers (Technical Capability) Regulations 2018* (UK) is before UK parliament and provides more details as to what these notices could require companies to do in relation to encryption and decryption.

17. Under the UK regime, where the operator has applied electronic protection (encryption), the operator will be required to be able to remove that where it is reasonably practicable.

18. In New Zealand, there is the *Telecommunications (Interception Capability and Security) Act 2013* (NZ). The primary obligation imposed under this legislation is the obligation for network operators, meaning those who operate or own telecommunications networks in NZ, to make sure their networks and services have full interception capability.

19. In the context of encryption services in New Zealand, the relevant operator needs to be able to decrypt messages where the operator itself has applied the encryption. Another section requires both network operators and telecommunication service providers to provide

assistance to law enforcement agencies who obtain warrants. That assistance in certain circumstances requires the removal of encryption where the operator/provider itself has applied the encryption.

Criticisms of the UK and New Zealand regimes

20. The UK legislation covers a broad range of surveillance rights given to the government, so it is sometimes referred to as the 'snooper's charter'. There is quite a bit of criticism of that Act that is unrelated to the encryption/decryption provisions specifically.

21. Legislation of this type (that is dealing with surveillance) always involves a balancing of the rights of privacy of individuals as against the rights of law enforcement agencies. There must be balance between keeping individuals happy in the sense that they are free from surveillance versus the need to ensure that law enforcement agencies have sufficient powers to prevent and prosecute breaches of law.

22. Another criticism is the cost issues. Both the UK and the NZ legislation impose obligations to take particular network action which could potentially be very expensive.

23. The UK legislation is also criticised for being too vague. It is quite difficult, particularly in the UK in the absence of any technical capability notices being issues as of yet, to work out what it is that operators may actually need to do. This creates difficulties for those who may be subject to the legislation.

24. Another area of criticism relates to compliance. These laws may require companies to do things that are not practically possible. It may also require entities to take action that will actually prejudice the rights of individuals and corporates who use encryption for legitimate business purposes such as for banking or for transmitting confidential information. The following paragraphs look at some of these issues in more detail.

25. The regulation that relates to technical capability notices purports to require operators to take action that is reasonably practicable, but it is difficult to work out what this actually means. The Secretary of State must consider costs before issuing a notice, but how much would an operator need to spend before it became not reasonably practicable for that operator to implement what was required by the Secretary of State? This also raises the question that if the solution imposed to allow decryption would prejudice legitimate uses of a particular service, does that mean it is not reasonably practicable (see also next paragraphs)? It is probable that the UK Courts will be looking at these issues fairly soon.

26. The most common criticism of this type of legislation is that the only practical way in which this legislation could work would be for technology companies to include back doors in their

products. For a back door to exist in the context of encryption, services such as WhatsApp, you would need a duplicate of the private key. The duplicate key would allow the company/provider of the service to decrypt messages that were sent.

27. The big problem that technology companies and commentators have in relation to back doors is that if law enforcement can walk through them, then obviously criminals can as well. This is problematic because legislation should not create a greater degree of risk for the community to solve a problem like encryption.

28. Another common criticism is that if back doors are used for common systems like WhatsApp, criminals will simply migrate to other systems.

29. These sorts of criticisms discussed above are currently also being raised in relation to the Australian legislation proposal. However, short of actually seeing the legislation, it is difficult to know which issues might create problems or whether the government will find a way of addressing those issues.

Other potential concerns with the proposed legislation

30. There are lots of other questions about the legislation. For example, will the government try to impose obligations on technology companies that provide messaging services that are encrypted, or will the class of regulated entities be broader than this? There is also the question of what communications the new legislation will apply to.

31. The former Attorney-General has said that the scope of the warrants that may be obtained to access communications won't be expanded, but whether this is actually the case is uncertain. As is the case in NZ and the UK, it is also not clear what the government will require companies to do. The Australian government has said that companies will not be required to introduce back doors, but if you need to do all that is reasonably practicable to assist in decryption, what that will require companies to do is still unclear.

32. Another interesting point is the extraterritoriality issues and cross-jurisdictional related issues with this legislation. For example, will the legislation purport to cover only Australian companies or companies operating in Australia? One would think not because that would limit the effectiveness of the legislation, but this then raises the issue of how the government will ensure that it can enforce this legislation at a global level.

33. Another potential concern is that if law enforcement do obtain access to decrypted communications under the new legislation, who will they be able to pass this information on to?

34. Governments and politicians tend to react to problems by suggesting legislation, but sometimes legislation is not the answer. For legislation to actually work, it needs to be able to achieve its aims and there are real concerns that this proposed legislation will not be able to achieve the aims the government is seeking.

35. It is difficult to see how telecommunications and technology companies will comply with any new law in a way that does not prejudice legitimate users of encryption technology. There is a distinct possibility that those who use encryption technology for nefarious purposes will find a different way of getting around the legislation, for example by downloading and using encryption software, and so on.

Preparation by technology companies now

36. It is difficult for technology companies to do anything practically in terms of their networks and services now, to ensure they are in a position to comply with the new legislation, because it is still unknown what the legislation will require. However, it is important that those companies do engage with the government in relation to the form of any potential legislation in a constructive and practical manner.

37. It has been publicly reported that the former Attorney-General met with quite a number of technology companies to work out the details of what would be sensible in this legislation. The community in general should definitely engage in any public consultation processes when the draft legislation is available.

BIOGRAPHY

Angela Flannery

Partner at Holding Redlich, Sydney

Angela is a partner in Holding Redlich's national Corporate and Commercial group. Angela has more than 20 years' experience as both a partner in private practice and in senior Commonwealth Government roles. She has broad ranging commercial law expertise, with a particular focus on telecommunications, media and technology (TMT) law. Angela has extensive knowledge of the regulatory framework governing the communications sector in Australia, including issues relating to telecommunications infrastructure, consumer regulation (including privacy) and the changing regulation in the media and content areas.

Karen Lee

Principal at Legal Know-How, Sydney

Karen is the principal at Legal Know-How. Karen has 20 years' experience in banking and financial services law, and specialises in regulatory compliance and legal knowledge management. Before founding Legal Know-How in 2012, Karen's experience included over 6 years spent in-house in leadership roles, and over 4.5 years spent focused on legal documentation, precedents and knowledge management at a top-tier Australian firm and a magic circle global firm.

BIBLIOGRAPHY

Legislation

Telecommunications (Interception and Access) Act 1979 (Cth)

Telecommunications Act 1997 (Cth), s 313

Investigatory Powers Act 2016 (UK)

The Investigatory Powers (Technical Capability) Regulations 2018 (UK)

Telecommunications (Interception Capability and Security) Act 2013 (NZ)