Opinion Piece

Law Council
OF AUSTRALIA

15 December 2018

Opinion: Encryption laws poorly executed, need further consideration

In the last hour, of the last day of Federal Parliament this year, unprecedented encryption access laws were rammed through the Senate.

This occurred despite politicians knowing that serious problems still exist.

The measures are complex, seemingly targeted, and to the everyday person, possibly of little consequence.

But they are some of the most far-reaching laws of their type introduced in the world and should be taken seriously by all Australians – they impact our most basic rights.

The Law Council of Australia, the voice of the legal profession, supports the purpose of the laws to keep us safe from the horror of terror attacks. But we believe that in the rush to get the legislation enacted it has been poorly executed.

This could have serious unintended consequences and there is a real risk these laws could be used for purposes outside protecting our national security.

The legislation's capabilities can be exercised in relation to any crime with a maximum penalty of three years' jail or more – a low threshold that sets a very broad scope.

Before they passed, the Law Council submitted these laws should only apply to crimes carrying a seven-year plus maximum prison term and should be specific to particular crimes, such as terrorism and child exploitation offences.

In the current form, however, these laws could, in theory, be used to target people suspected of relatively minor offences, such as theft.

The encryption access bill gives our law enforcement and intelligences agencies unprecedented powers to exercise intrusive covert powers, accessing messages sent over encrypted messaging software and intercepting communications.

The need for a warrant is also potentially side-stepped, as law enforcement agencies now have the power to issue 'technical assistance requests' or 'voluntary assistance requests' to designated communications providers to access and decrypt an individual's private information.

Further, individuals – such as IT experts – could be held and forced to provide compulsory assistance without the safeguards necessary for detention, including being able to contact a lawyer. There is also a stark lack of assurances for lawyers, with a failure to protect the integrity of legal professional privilege.

It is the Law Council's firm view our law enforcement agencies should not be allowed to bypass the need to obtain a warrant when accessing information via encrypted or intercepted communications.

The Australian Government's rushed and politicised encryption access legislation, as it stands, is not fit for purpose and poses a real risk to the rule of law.

Next year Parliament has the chance to immediately revisit these laws and ensure they get them right.

The consequences of not doing so can impact us all.

Morry Bailes
President, Law Council of Australia

Contacts:

Patrick Pantano
P 02 6246 3715
E Patrick.Pantano@lawcouncil.asn.au

Anne-Louise Brown
P 0406 987 050
E Anne-Louise.Brown@lawcouncil.asn.au