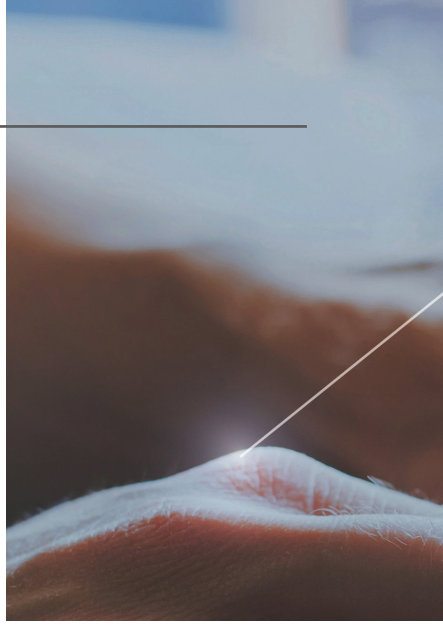
By Dennis Miralis, Nyman Gibson Miralis



ENCRYPTION LAW

The Key Changes Made to Australia's Encryption Laws

Dennis Miralis speaks to us this month about Australia's encryption laws. He touches on what has changed and the impact it has had.

Encryption laws have been a hot topic in recent times. What have been the key changes in Australia?

On 8 December 2018, Federal Parliament passed the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 ('Bill').

The Act provides for the facilitation of covert access to data for the purposes of disrupting and investigating criminal activity, as well as establishing a framework to facilitate lawful assistance from communications providers.

Do the changes introduced by the Bill give authorities 'back door' access to data?

Whether 'back door access' is the correct technical term or not, the fact is that the changes essentially give law enforcement authorities unrestricted access to data. The Bill allows law enforcement agencies to request or order a designated communications provider to provide technological assistance including, but not limited to: removing encryption/ electronic protection, providing technical information and facilitating access to devices and the data stored on them. Assistance orders fall under three categories:

1) Technical assistance request (TAR) – a request asking a provider to voluntarily provide data or assistance in relation to criminal investigations or matters of national security.

2) Technical assistance notice (TAN) – similar to a TAR except that it is an order, rather than a request.

3) Technical capability notice (TCN) – which mandates that a communications provider establish new capability to intercept and decrypt communications that would otherwise be encrypted.

What other key provisions are included in the Bill?

The Bill amended the Surveillance Devices Act 2004, allowing law enforcement agencies to obtain computer access warrants while investigating certain federal offences. It also allowed Australia's domestic spy agency, ASIO to intercept communications under a computer access warrant, and to undertake any activities necessary to conceal that such

Dennis Miralis

Dennis Miralis is a leading Australian defence lawyer who practices in the following areas of complex domestic and international criminal law; white-collar and corporate crime; bribery and corruption; cybercrime; money laundering; serious fraud; worldwide asset forfeiture; transnational crime; extradition; Interpol Red Notices; anti-terrorism law; national security law and encryption law.

He appears in all courts throughout Australia and regularly travels outside of Australia to advise in complex international criminal law matters.

Contact

Dennis Miralis, Partner
Nyman Gibson Miralis
Level 9, 299 Elizabeth Street, Sydney NSW 2000, PO BOX 21147, World Square, NSW 2002, DX 11543, SYDNEY DOWNTOWN
Tel: +61 2 9264 8884 | Fax: 9264 9797
Mob: 0414 933 168 | ngm.com.au

NYMAN GIBSON MIRALIS
Criminal Defence Lawyers and Advisors est. 1966

By Dennis Miralis, Nyman Gibson Miralis

access was made, even after the warrant has expired.

Other key provisions include increasing the scope of data collection by allowing such collection to occur remotely, as well as expanding police powers by allowing them to compel a person specified in an assistance order to provide on-the-spot access to data held on a device that may contain evidence useful in an investigation.

Several broad and discretionary powers were introduced to facilitate greater access to data and communications which may be relevant to police investigations.

What are the legal tests to be applied to requests and orders?

The test to be applied varies depending on the specific request or order sought.

For a TAR, the request must be made pursuant to the enforcement of criminal laws and laws imposing pecuniary penalties, either in Australia or in a foreign country, or if it is in the interests of Australia's national security, Australia's foreign relations, or Australia's national economic well-being.

A TAR may also cover matters that are incidental or ancillary to such matters, therefore it appears there is a low threshold for getting such a request granted.

> **"Several broad and discretionary powers were introduced to facilitate greater access to data and communications which may be relevant to police investigations."**

For TANs and TCNs, the test is the same as the TAR test, with additional conditions that the requirements of the notice be reasonable and proportionate, and that compliance with the notice is practicable and technically feasible.

What are the key considerations in applying these tests?

The Director General of Security or the Chief Officer of an interception agency must have regard to a number of considerations, including: the interests of national security and law enforcement; the legitimate interests of the designated communications provider to whom the notice relates; the objectives of the notice; the availability of other means to achieve the objectives of the notice; AND the legitimate expectations of the Australian community relating to privacy and cybersecurity, and any other relevant matters.

What are the penalties for non-compliance?

A person who has been compelled to provide data or assistance under a computer access warrant and fails to do so may face up to 10 years imprisonment, a fine of up to $126,000 (600 penalty units), or both.

A carrier or carriage service provider that fails to comply with an assistance order (either a TAN or TCN) could face a fine of up to $250,000 for a body corporate or $50,000 for others. A designated communications provider (other than a carrier or carriage service provider) that fails to comply with an assistance order could face a fine of up to $9,999,990 (47,619 penalty units) if it is a body corporate, or $49,980 (238 penalty units) for others.

The penalties for non-compliance are severe, demonstrating the seriousness of these offences.

> **"Concerns have also been raised relating to the impact on procedural fairness due to the reversal of the evidential burden of proof through the introduction of offence-specific defences, as well as the significant penalties for non-compliance with assistance orders."**

Expert Insight

By Dennis Miralis, Nyman Gibson Miralis

What were the main arguments raised against the introduction of this bill?

There are arguments that the breadth and significance of powers conferred on the Executive would only be subject to limited parliamentary oversight; the Executive is granted with broad discretionary powers, some of which have been exempt from judicial review.

Concerns have also been raised relating to the impact on procedural fairness due to the reversal of the evidential burden of proof through the introduction of offence-specific defences, as well as the significant penalties for non-compliance with assistance orders.

Apple raised concerns relating to ambiguity, as they submitted that the scope of the powers introduced is ill-defined and could potentially lead to greater encroachments on individual privacy than perhaps initially expected.

It has also been posited that the breadth of powers to remove things from premises and to conceal any actions taken under a computer access warrant are vague and potentially invasive, especially as this power continues even after a warrant has expired.

What is the stance of Nyman Gibson Miralis on the bill?

The Department of Home Affairs recently sought public consultations on the Bill, and Nyman Gibson Miralis made a submission to the Department.

In certain circumstances, access to encrypted communications may be a legitimate means for law enforcement to disrupt or investigate serious crime. However, Nyman Gibson Miralis took the view that the Bill does not offer a reasonable approach to this issue and would have profound implications for privacy within Australian society.

The Government may be correct in its claim that the Bill is not aimed at the creation of 'backdoors' into private communications, but this is merely because, as it stands, the Bill empowers the Government to demand the key to the front door.

What were the key elements of the submission by Nyman Gibson Miralis?

In our submission, Nyman Gibson Miralis emphasised the importance of human rights to this issue. In particular, there has been a great deal of discussion by international bodies and experts on the proper limits that should be placed on government actions in the field of communications access in order to ensure respect for citizens' right to privacy.

We also took issue with the Bill's proposal for government officials to compel encryption providers to assist in accessing personal communications. In the firm's submission, it was contended that any such authority should only be granted to judicial authorities (in a similar manner that already exists under section 3LA of the Crimes Act 1914). This would ensure independent oversight of such actions and provide consistency with established procedures for analogous situations.

Furthermore, although the Government has asserted that such notices would be the subject of reporting requirements and be challengeable through judicial review, Nyman Gibson Miralis took the view that the proposed mechanism is inadequate, and does not provide sufficient transparency and accountability.

Specifically, reports on the issuance of the notices contemplated in the Bill should be required to include more than bare numbers (as proposed). Rather, details of the nature of the alleged offences connected with the exercise of such powers in the case and information about the basis upon which access to the communications was sought should also be publicised.

Further, by focussing only on the agency providing carriage of communications, persons subject to government monitoring are essentially cut out of the process. This would effectively render their right to challenge the government's action as being of little value. Consequently, any legislation should provide for affected individuals to be properly notified when such action is taken. **LM**

> **"In particular, there has been a great deal of discussion by international bodies and experts on the proper limits that should be placed on government actions in the field of communications access in order to ensure respect for citizens' right to privacy."**