

Committee Secretary
Parliamentary Joint Committee on Law Enforcement
PO Box 6100
Parliament House
Canberra ACT 2600

By email also: le.committee@aph.gov.au

Submissions to the Inquiry into the impact of new and emerging information and communications technology on Australian law enforcement agencies

Nyman Gibson Miralis

1. This submission is made to the Parliamentary Joint Committee on Law Enforcement with respect to their Inquiry into the impact of new and emerging information and communications technology on Australian law enforcement agencies.
2. Nyman Gibson Miralis is a leading Australian criminal law firm specialising in international criminal law and has acted and advised in matters involving encryption enabled technology in Australia connected to criminal investigations and Proceeds of Crime proceedings (POCA)
3. Nyman Gibson Miralis has also engaged with various Australian authorities and Departments concerning encryption enabled devices on behalf of encryption suppliers and distributors.
4. In particular, our submission will focus on the role and use of encryption, encryption services and encrypted telecommunication devices.



SYDNEY OFFICE **ph** +61 2 9264 8884 **a** Level 9, 299 Elizabeth Street, Sydney NSW 2000 **dx** 11543 Sydney Downtown
PARRAMATTA OFFICE **ph** +61 2 9633 4966 **a** Suite 8, Level 2, 154 Marsden Street, Parramatta NSW 2150 **dx** 8280 Parramatta
abn 89 340 323 906 **w** ngm.com.au

Introduction

5. The rise of new and emerging information and communications technology has highlighted the need for increased cyber security namely in the form of encryption.
6. Accordingly, we recognise the potential for encryption devices, technologies, and services to be misused particularly by those engaged in serious or organised crime, and to diminish the investigative capabilities of Australian law enforcement.
7. However, despite such concerns, we contend that there are sufficient legal mechanisms that are underutilised by law enforcement to adequately address these issues.. Going beyond the current mechanism would likely result in excessive state surveillance, significant intrusion on people's right to privacy and threaten the cybersecurity of ordinary citizens.

Encryption is not a crime

8. Until Parliament legislates otherwise, supplying encryption services and devices in Australia is not illegal.

Law enforcement present approach to encryption services- disruption model

9. There appears however to be an unstated assumption amongst international law enforcement agencies that those who use particular encryption services must be involved in criminal as opposed to legitimate activity. To date very little evidence based research has been presented to support this contention.
10. Consequently, as a means to disrupt the supply of encrypted telecommunication devices such as phones, law enforcement generally employs "disruption techniques" to the supply chain, to seek prevent the targeted phones from being distributed to members of the public.
11. Often this can be achieved by bringing charges contrary to the proceeds of crime offence provisions under both the Commonwealth or State legislation. (money laundering provisions) due to the suppliers of encrypted communication devices being in possession of cash - typically profits from selling their encrypted devices.
12. Additionally, such phone suppliers are often prohibited from mainstream banking and the agents selling these devices exposed to regular questioning and surveillance. The users of such devices remain of interest to law enforcement, because of the assumption that there is no legitimate reason for anybody to use high grade encryption to communicate.
13. Such an approach has the effect of deterring members of the Australian public from using encryption devices notwithstanding that these devices have not been criminalised, prohibited or regulated.
14. To the extent that it is perceived that this kind of law enforcement activity is necessary (until such time as there is formal legal redress concerning the use of encrypted telephones) it would be desirable that it be the subject of open public debate, given the capacity of such activity to unduly infringe on personal liberties, including the right to anonymity and privacy.

Genuine reasons for encryption and striking the right balance

15. We submit that there are many legitimate reasons why ordinary people use encryption services, for example:
- a. Protecting sensitive personal data, including financial and identity information to prevent becoming a target of cybercrime committed by malicious actors;
 - b. Businesses wanting to safeguard commercial secrets.
16. We also contend that encryption is essential to protecting the right to privacy and freedom of expression without fear of persecution. Thus, any attempt to enable surveillance by compromising encryption will not only undermine cybersecurity for all users but will severely affect a number of vulnerable parties who rely on secured communication services such as:
- a. Human rights activists who work in closed countries where surveillance is prevalent and need encryption to securely communicate and report human rights abuses committed by the Government in question;
 - b. Whistle-blowers who disclose governmental or corporate wrongdoing; and
 - c. Journalists trying to safeguard the identity of their sources.
 - d. Legal practitioners communicating legally privileged information.

No prohibition or limitation on Encryption

17. We strongly submit that there should be no further prohibition or limitation (including a blanket ban) placed on encryption under Australian law.
18. It is submitted that if the law were to further compromise encryption in favour of surveillance, such change would be an overreach and it would offend Australian democratic principles including the freedom of speech and association, and values of openness and transparency.
- a. A recent example of such overreach is the Turkish Government's pre-trial detention of 40,000 people who were allegedly using an encryption messaging service favoured by the Gulen movement.¹ This pervasive view amongst many Sovereign Governments, that encryption should be banned and criminalised is wrong. Such a view is also disproportionate to the public interest benefits that encryption provides as previously noted.
19. Thus, we submit that the misuse of the protection that encryption offers (including using encryption to conceal criminal activity) is not reason enough for the Australian Government to restrict the general population's access to encryption devices and services.

Legal mechanisms in dealing with problems associated with encryption

20. Section 3LA of the *Crimes Act 1914* (Cth) (**3LA orders**) provides significant powers of decryption to Australian law enforcement officers. Namely, it provides officers the power to compel a person to reveal their private encryption keys, personal

¹The Guardian, *Turks detained for using encrypted app 'had human rights breached'* (11 September 2017) <<https://www.theguardian.com/world/2017/sep/11/turks-detained-encrypted-bylock-messaging-app-human-rights-breached>>.

identification numbers or passwords, to access information held on a computer that is reasonably suspected of storing evidential material.

- a. A failure to comply with the law enforcement officer's request is punishable by up to six months' imprisonment.
21. We submit that 3LA orders proportionately and adequately deal with any concerns that law enforcement have regarding encryption including its potential misappropriation by criminals.
 22. In our view, 3LA orders strike the right balance between preserving the general public's use of encryption services and the need for law enforcement to access pertinent information relevant to the suspected commission of a criminal offence.
 23. Furthermore, 3LA orders can be challenged through judicial review.
 - a. This further provides a layer of accountability especially for innocent parties who happen to be subject to an application for a 3LA order.

International cybercrime and extradition

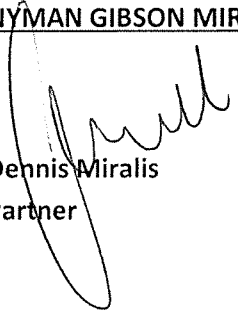
24. We would like to make an additional submission concerning the increasing detection of criminal activity in the areas involving emerging information technologies including encryption devices and its potential impact on Australians who may be charged with such activity by foreign law enforcement.
25. It is contended that there is currently inadequate protection afforded to Australian citizens under Australian extradition law.
26. We recommend that Australia should consider legislating a 'forum bar' similar to section 83A of the Extradition Act 2003 (UK) ('EA'). Under s 83A(1) EA, extradition from the UK to another country 'is barred by reason of forum if the extradition would not be in the interests of justice.' There are specific matters relating to the 'interests of justice' that a Judge must consider under s 83A(3) EA.
27. The purpose of the forum bar is to stop the extradition of vulnerable British defendants when UK Courts could provide a more appropriate 'forum' to deal with their case.
 - a. In the case of *Lauri Love v The Government of the United States of America*,² alleged hacker Lauri Love was barred from extradition when the UK High Court of Justice ruled that it would be contrary to the 'interest of justice'.³ Among other things, the High Court of Justice decided that:
 - i. Even though it was more desirable for Love to be extradited given all the witnesses were located in the US, substantially more weight was given to his person connections to the UK.
 - ii. There was strength in the significance of Love's connection to his family who deliver the necessary care, medical treatment and stability he needed which could not be provided in the US. Love suffered from Asperger's, severe depression and Eczema (which adversely affected his mental state).

² [2018] EWHC 172 (Admin).

³ S 83A Extradition Act 2003 (UK).

28. Thus, we submit that a similar forum bar should be inserted into s 19 of the *Extradition Act 1988* (Cth) as it is likely that Australians will be increasingly exposed to extraditions requests by foreign governments alleging offences that have employed emerging technologies.

NYMAN GIBSON MIRALIS



Dennis Miralis
Partner

NYMAN GIBSON MIRALIS



Phillip Gibson
Partner
Accredited Specialist Criminal Law