SUBMISSION

Independent National Security Legislation Monitor (INSLM)

Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA Act)

October 2019

Simone Denereaz

Private Citizen, Australia

INSLM Submission, October 2019

Summary of Observations

1. The TOLA Act was rushed through the democratic Parliamentary process and incorporates limited PJCIS public inquiry outcomes and PJCIS (LNP & Labor) democratic input
2. The TOLA Act legislates access to target private data for broad purposes. Similar methods have been used for surveillance by Communist regimes to suppress political opposition
3. TOLA Act access is not yet compatible with a democracy. Democracies have Media Freedom legislation and Human Rights Charters which ensure a healthy rule of law can be maintained
4. TOLA Act style access has historically facilitated mass surveillance and breakdowns in the rule of law
5. TOLA Act access could slow progress and development. It could be used as both an enforcement and a security tool
6. The TOLA Act procedures do not consider diversity and inclusion

Background

The TOLA Act is a recent technology, access and assistance law which was passed in 2018 and amends various Australian laws, including the Crimes Act 1914. The TOLA Act is a new and anomalous addition to Australian security legislation. The TOLA Act entitles law enforcement and security agencies to force a technical, cybersecurity or telecommunication expert to access data on a mobile phone or electronic device in secret, for legislated broad reasons including 'in Australia's best interest'. If necessary, the expert must make a tool to break encryption. This can occur at any time for approved time periods to investigate potential crime in Australia or a foreign country which would result >3 years in prison, or to protect Australia's best interests for various national security, national economic well-being or foreign relation reasons. The Federal Attorney General and Communications Minister, and Heads of security agencies and law enforcement bodies approve technical requests for access, depending on their application. If a warrant is required it is approved by qualifying assessors as specified by legislation such as an ex-judge, judge or AAT member. The Commonwealth Ombudsman is notified of technical request approval and changes.

Introduction

The TOLA Act was passed in December 2018 by the Australian Parliament. The six observations below have been prepared for this INSLM TOLA Act review submission. Each observation articulates concerns which should be considered to ensure the current enacted version of the TOLA Act being reviewed by INSLM is not used incorrectly to harm citizens in the short and long-term future and to ensure adequate protections are in place to protect Australia's position and reputation in the global order as a democracy.

Discussion

Observation 1: The TOLA Act was rushed through the democratic Parliamentary process and incorporates limited PJCIS public inquiry outcomes and democratic input

The PJCIS process is an important democratic parliamentary process which reviews national security legislation and requests public submissions and holds public inquiries. The notice periods for TOLA Act submissions and public inquiry participation were short and citizen (including business and academia) contribution, representation and expenses incurred were contributed on a voluntary basis. PJCIS is presently comprised of Labor and LNP MP's. It is likely that the TOLA Act would be different if this process had been completed. A single PJCIS redrafting event is low for complex and highly consequential legislation.

Observation 2: The TOLA Act legislates access to target private data for broad purposes. Similar methods have been used for surveillance by Communist regimes to suppress political opposition

The TOLA Act could be used to suppress political opposition and victimize citizens. Qualifying assessors should be independent and not influenced by politics. The TOLA Act amends the Crimes Act 1914. Consideration should be given to how a range of political parties could use the TOLA Act in the short and

long-term future in Australia and whether Communist style censorship and suppression of political opposition could occur. TOLA Act access should be used sparingly in functional democracies and specific safeguards added to ensure use is limited.

Observation 3: TOLA Act access is not yet compatible with a democracy. Democracies have Media Freedom Acts and Human Rights Charters which ensure a healthy rule of law must be maintained

The present version of the TOLA Act within Australia's current domestic legal framework increases the risk of invasive surveillance occurring without adequate accountability, limitations and oversight. The security and law enforcement agencies who use the TOLA Act and the Government can achieve their goals with very few risks or consequences. All TOLA Act related information is secret and any media reporting about the TOLA Act is illegal and could result in prison sentences of 10 years. There are no explicit Commonwealth human rights protections for Australian citizens. In the absence of a Media Freedom Act and Human Rights Charter, specific media freedom and human rights protections should be included in the TOLA Act.

Observation 4: TOLA Act style access has historically facilitated mass surveillance and breakdowns in the rule of law

If TOLA Act access is used for censorship and to suppress political opposition, the rule of law could subsequently breakdown. The Australian people will not know if this has or does occur. The TOLA Act in its current form could suppress political opposition. Media oversight is not allowed. Human rights are not required. The TOLA Act could be misused in a variety of ways for government personal and political gain.

Observation 5: TOLA Act access could hamper progress and development. It could be used as both an enforcement tool and a security tool

TOLA Act access and corresponding operations, particularly for national interest or political purposes could take precedence over progress and development. It should be considered whether limitations would stimulate growth in the technology sector (which relies on encryption) and other industries. Adequate whistle-blower's legislation could add safeguards for technology, cybersecurity and telecommunication experts. Exploits designed for surveillance purposes could be resold or reused. Protections and limitations for technology, cybersecurity and telecommunication experts required to give help to the Government such as anonymity, independence and limitation of request number should be considered.

Observation 6: The TOLA Act procedures do not consider diversity and inclusion

TOLA Act access requires the involvement of Ministers, qualifying approvers (including an ex-judge and AAT member), Home Affairs, law enforcement and security agency officials and staff, and technical cybersecurity and telecommunication experts. These groups are generally comprised of a high percentage of male employees. The impact of incorporating additional diversity and inclusion into the TOLA Act procedures should be considered.

Conclusion

In practice, the TOLA Act provides procedures which could be described as a master-key for an Australian property where technology or data is housed, and an invisibility cloak to wear in there to take whatever is required. The potentially dangerous and coercive behaviour which could result from these powers is wide in scope. Whilst the TOLA Act may be immediately functional and common sense can be applied to understand its use, consideration should be given as to how potential misuse can be limited, independence of security agencies and law enforcement remains free of political motivations, how public inquiry and PJCIS input can be incorporated and how the inclusion of media freedom and human rights protections are necessary for democracy.

INSLM Submission End