19 January 2021

UPDATE
2021 Quick start: Australian Cyber Security Policy

This update provides a New Year recap of late-breaking developments in Australian national security policy in 2020.

You can jump to those that interest you by clicking the relevant link:

Contents

1. Changes to Foreign investment rules

On 10 December 2020 parliament passed the changes to Australian foreign investment laws outlined in our 17 August 2020 Update. The proposed changes became law 1 January 2020. In summary:

- Monetary thresholds for screening foreign investments have been reintroduced except for investments by foreign governments and "notifiable national security actions" (**NNSAs**) where the threshold is zero. NNSAs involve investment or starting a "national security business" or national security land. The definition of "national security business" includes critical infrastructure, telecommunications and business that supply the military, defence and/or national intelligence.
- The Foreign Investment Review Board now has call-in powers for investments not otherwise subject to review.
- A consolidated register of foreign owned assets is created.
- The Senate added a requirement that a report on the impact of the new laws on foreign investment in Australia be provided to the Treasurer by the end of 2021.

2. New online safety legislation

On 23 December 2020, the Department of Infrastructure, Transport, Regional Development and Communications released for consultation an exposure draft of a new Online Safety Act.

The new legislation would introduce the following key changes:

- New powers for regulating content, takedown and website blocking for the eSafety Commissioner.
- Cyber-bullying scheme expanded from social media to online services supporting games, websites, messaging services, hosting services.
- A reduced online content takedown deadline of 24 hours.
- Power to require removal of takedown material from search engines and app stores.
- Basic Online Safety Expectations (BOSE) to be imposed on digital products and services and be set in law.
- New mandatory reporting obligations for "online harms" and compliance with BOSE.
- A requirement for industry to create "new and strengthened" industry codes for control of online content within 12 months.

The consultation period closes on 14 February 2021.

3. Surveillance Legislation Amendment (Identify and Disrupt) Bill

On 3 December 2020, the Minister for Home Affairs introduced a Federal Parliament the *Surveillance Legislation Amendment (Identify and Disrupt) Bill* (**IDB**). On 8 December 2020 the IDB was referred to the Parliamentary Committee on Intelligence and Security (**PJCIS**).

The IDB proposes to give law enforcement and national security agencies new powers to be used where the disruption of data held in a target computer is likely to substantially assist in frustrating the commission of one or more relevant offences. It is proposed that law enforcement and national security agencies have the power to enter premises, disrupt the relevant data, and, copy, delete or altar other data on the target computer and or in transit as well as "any other thing reasonably incidental to the above".

Submissions to the PJCIS close on 12 February 2021

4. New framework for Security of Critical Infrastructure

The *Security of Critical Infrastructure Act 2018* (**SoCIA**) requires the owners of certain nominated ports, electricity, water and gas infrastructure of scale, and other infrastructure nominated by the Minister, to be placed on a secret register and required to report ownership and operational details. Infrastructure assets may be subject to investigative powers and Ministerial direction. After a short consultation, on 10 December 2020 the *Security Legislation Amendment (Critical Infrastructure) Bill* (**Bill,**) with minor amendments from the exposure draft, was introduced into the Federal Parliament.

The Bill expands SoCIA to cover assets in the communications, data storage and processing, financial services and markets, energy, healthcare and medical, higher education and research, food and grocery, transport, space technology and the defence industry. Critical assets in these sectors can be made subject to the existing regulatory framework and/or required to adopt and maintain a risk management program, mandatory reporting of serious cyber incidents and/or comply with an annual reporting requirement. The criteria that determine whether or not an asset is critical are different for each sector but, generally, do not set a high bar.

Critical assets in each sector can be made subject some or all of the regulatory framework according to Ministerial rules or Ministerial declaration. The test for making a rule nominating a critical asset for regulation is that it is "necessary or convenient to be prescribed for carrying out or giving effect to this Act". The Minister may make a relevant declaration after consultation.

Having regard to interdependencies with other critical infrastructure assets, the Minister may declare a critical infrastructure asset a system of national significance (**SoNS**). A SoNS is automatically subject to an incident response planning obligation, can be required to participate in cyber security exercises including undertaking an evaluation and issuing a report in relation to the incident planning exercise, undertaking a vulnerability assessment, delivering events-based reporting of system information and/or installing system information software.

If a cyber security incident has occurred, is occurring, or is considered imminent, the incident is considered likely to have an adverse impact on a critical infrastructure asset including a material risk of serious prejudice to the social or economic stability of Australia or its people, the defence of Australia or national security, and no existing regulatory system could be used to provide a practical and effective response to the incident, the Minister may authorise an information gathering direction, a direction to do a specified act or thing, or require a government agency to intervene in relation to the protection of the asset.

On 18 Dec, the Bill was referred to the PJCIS with submissions due by 12 February. The PJCIS page on the Bill is here. It is expected that the PJCIS will complete its review by early May and the Bill may become law as soon as July 2021. The practical impact of the new law will depend on the sector rules and any ministerial declarations. It is anticipated that there will be a consultation process on the development of sector specific rules following passage of the legislation.

5. Review of the Privacy Act

On 30 October 2020, the Attorney-General's Department published an issues paper seeking guidance in relation to a review of the ***Privacy Act 1988***. Key proposals listed in the consultation paper include:

- whether the definition of personal information is adequate to protect technical information.
- whether changes should be made to protect de-identified, anonymized and pseudonymized information.
- amendment or removal of the small business exemption.
- the appropriateness of exemptions for employee records political parties and journalists.
- improvement of notification requirements.
- adequacy of the existing approach to individual consent.
- the possible introduction of pro-consumer defaults positions.

- the introduction of requirements for obtaining consent in relation to the use of personal information relating to children.
- the privacy impact of IOT devices.
- the application of the act to inferred information including sensitive information.
- the adequacy of security requirements imposed by the Act.
- whether a right of erasure should be introduced.
- the adequacy of Australian Privacy Principal 8 and cross-border disclosure rules.
- the role of the Office of the Australian Information Commissioner and the enforcement regime.
- whether a direct right of action and/or a statutory tort for breach of privacy should be introduced.
- the impact and adequacy of the notifiable data breach is regime.

Submissions closed on 29 November 2020 and can be reviewed here.

6. Digital Identity framework

The Digital Transformation Agency (**DTA**) maintains the Trusted Digital Identity Framework (**TDIF**) for use by Commonwealth agencies and organisations. On 16 November 2020, the DTA published a Background Paper and a Discussion Paper on proposed TDIF legislation. Submissions closed on 18 December 2020

The scheme proposes the accreditation of participants by an operating authority established by statute. Accredited participants will be required to comply with operating rules and notify operating authority of matters related to security and fraud impacting the system. Digital identities will be distributed between accredited participants. Digital identities will comprise the attributes of a person, but information obtained from the system cannot be used for profiling or accessing associated attributes. The proposed framework will comprise legislation, legislative instruments and the TDIF.

The consultation paper highlights a tension between providing a high degree of assurance through a relatively fixed scheme specified in legislation compared to a more flexible scheme where fundamental elements are set out in the TDIF and legislative instruments.

7. Richardson Review and response

The Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community prepared by Mr Dennis Richardson, former Director-General of Security, Ambassador to the USA and Departmental Secretary, was published by the Attorney-General on 4 December 2020. The government response was also published on that day.

The report is generally supportive of the existing regime but recommend a range of adjustments in 203 recommendations. Recommended changes include increased powers to collect information on Australian citizens, greater flexibility in using open-source information and "that the AGO (Australian Geospatial Organisation) should be established as a statutory authority before acquisition of a sovereign geospatial intelligence space capability, with the timing to be revisited as part of future independent intelligence reviews. There are many other significant recommendations.

Of particular note are:

- **Recommendations 75** :"*The Surveillance Devices Act, Telecommunications (Interception and Access) Act* and those parts of the *Australian Security Intelligence Organisation Act* governing the use of computer access and surveillance devices powers should be repealed and replaced with a new Act." This recommendation is supported by the government.

- **Recommendation 111**:"Under a new electronic surveillance Act, the Attorney-General should be given the power to require a company to develop and maintain a specified attribute-based interception capability. If such a capability has been developed, agencies should be able to obtain attribute-based interception warrants in cases where it will be practicable for the warrant to be executed." This recommendation would significantly expand government surveillance powers by removing the restriction that interception warrants be limited to particular services or persons. It is supported by the government.

8. Inquiry into extremist movements and radicalism in Australia

On 9 December 2020, the Minister for Home Affairs referred "the nature and extent of, and threat posed by, extremist movements and person holding extremist views in Australia" and related matters for consideration and report by the PJCIS. The brief raises a number of important cybersecurity issues for consideration including "the role of social media, encrypted communications platforms and the dark web in allowing extremists to communicate and organise".

The PJCIS has opened an inquiry and called for submissions by 12 February 2020.

9. Telecommunications Security Sector Reform Review.

On 4 September 2020 the PJCIS opened consultation on the network security obligation introduced into Part 14 of the *Telecommunications Act* 1997 in 2018 (**TSSR**). The primary TSSR obligation is that carriers and carriage service providers must do their best to "protect telecommunications networks and facilities owned, operated or used by the carrier or provider from unauthorised interference or unauthorised access…" to protect communication confidentiality and the integrity of networks and facilities. The PJCIS asked for comment in particular on the effectiveness of the regime, the adequacy of information sharing between government and industry and the adequacy of industry guidelines. Submissions closed on 27 November 2020.

10. Outcome of review of mandatory data retention

Since 2015, carriers and carriage service providers that have a service for carrying communications must retain a specified set of data relating to and arising from use of each such service. The data that must be retained includes details of the customer and the service, and in relation to each communication session, any relevant device, the source and destination, duration, and location subject to certain exclusions. The dataset must be retained for two years and information provided in the dataset must be provided to certain national security and law enforcement agencies if requested. This regime is subject to regular regular statutory review by the PJCIS. The PJS handed down its first review report on 28 October 2020.

The Report recommends the creation of national guidelines for operation of the scheme by enforcement agencies and makes a number of recommendations related to securing and protecting data stored by carriers and carriage service providers and disclosed to enforcement agencies. Of particular interest:

- a recommendation that the government clarify the meaning of the distinction between meta data and the content or substance of the communication.
- a recommendation that the mandatory data retention obligation be removed from IOT devices.
- an amendment to prevent organisations other than enforcement agencies from using statutory powers under other legislation including state legislation from obtaining access to retain data.
- Improvements to the reporting regime.

The government is yet to respond to these recommendations.

11. Action on the INSLM Report

The PJCIS is reviewing the *Telecommunications and Other legislation Amendment (Assistance and Access) Act 2018* (**TOLA**). The subject of this inquiry was referred to the National Security Legislation Monitor (**INSLM**) whose report is available here. The INSLM report recommends that the government create independent oversight as a condition of exercise of the powers introduced by TOLA. The INSLM's recommendations are in line with industry submissions but it is not certain that they will be adopted by the PJCIS or the government. The PJCIS was due to report on 20 September 2020 but has not been issued.

12. International production orders: Executive Agreement under the US Cloud Act.

As outlined in our Update of 10 March 2020, the PJCIS is reviewing legislation currently before federal Parliament to introduce a reciprocal scheme that would enable Australian law enforcement and national security agencies to issue "International Production Orders" (**IPOs**) directly to offshore electronic service providers that may hold information on offences committed against the laws of Australian. Submissions closed on 30 April 2020. No report has been issued. The implementation of the IPO scheme requires that Australia enter into an "Executive Agreement" with participating foreign country. The writer understands that the Executive Agreement between the USA and Australia is being progressed but will not be signed until after the legislation is passed. The legislation awaiting the PJCIS report. The Executive Agreement between the USA and the UK can be found here.

* * * *

Please contact me if you have any questions regarding these developments

patrick@patrickfair.com 0411361534

Level 26 1 Bligh Street
Sydney NSW 2000 Australia
L +61 2 8226 8584
M +61 (0) 411 361 534
F +61 2 8226 8899
E patrick@patrickfair.com
W www.patrickfair.com
Technology Law Pty Ltd.
ABN: 44 003 792 809