National Security and Tech: The New Decade

Patrick Fair, principal at Patrick Fair Associates, comments on the developments at the intersection of national security and tech between 2010-2019, and on what's on the agenda in this space for the next decade.

1. Introduction

Australia's national security regime has developed significantly over the last decade. The government introduced significant new powers to fight terrorism and a range of measures focused on identifying and protecting Australia from foreign interference. Some significant changes were made to respond to technological change while others aimed at making national security agencies and law enforcement more efficient and effective.

This short article provides an overview of the key national security changes introduced over the last decade and of the changes that are in the pipeline. In the conclusion, there is an outline of some of the issues that might drive further change.

2. The Decade Past: laws to fight terrorism

During the early part of the decade developments in Syria and Iraq and news that some Australians had travelled to fight with Daesh resulted in the introduction of the new penalties and expanded powers to address terrorism.

In 2010 the National Security Legislation Amendment Act 2010 amended a number of Acts to adjust treason and sedition offences, to clarify when an organisation advocates the doing of a terrorist act, to add powers to search premises in relation to terrorism offences, re-entry of premises in emergency situations, bail for terrorism and national security offences and more.

The Counter-Terrorism Legislation Amendment (Foreign) Fighters Act 2014 amended the meaning of 'terrorism offence' in the Crimes Act 1914, extended the power to arrest without a warrant and introduced the delayed notification search warrants, made a new offence of advocating terrorism, changed and extended the control order and preventative detention order regimes, and introduced stop, search and seizure powers relating to terrorism offences. The Act also introduced a new offence of 'publicly advocating genocide' to people inside or outside Australia, carrying a maximum sentence of seven years' imprisonment. ASIO was given a new questioning and detention warrants regime and changes were made to the Foreign Evidence Act 1994 to provide greater discretion in admission of foreign material in terrorism-related proceedings. You might recall the public controversy over the new offence of disclosing information relating to warrants or execution of a warrant introduced to the Criminal Code as 3 HA due to concern regarding the impact on reporting of news.

On 11 December 2015 assent was given to the Australian Citizenship Amendment (Allegiance to Australia) Act 2015 which describes certain terrorist related activity by a dual citizen as constituting a renunciation of Australian citizenship and/or giving rise to a ministerial power to cancel Australian citizenship.

On 2ɔ November 2016 the Counter-Terrorism Legislation Amendment Bill (No.1) 2016 received assent introducing further extensive changes to the Criminal Code control order provisions including adding provisions to effectuate the use of tracking devices on persons the subject of control orders and expanding powers to monitor compliance.

On 7 December 2016 the Criminal Code Amendment (War Crimes) Act 2016 received assent. This Act amends Division 268 of the Criminal Code to align Australian domestic law with international law in relation to the treatment of members of organised armed groups in non-international armed conflict. The Act amends Division 268 of the Criminal Code to give effect to Australia's obligations as a party to the Rome Statute of the International Criminal Court.

Also on 7 December 2016 assent was given to the Criminal Code Amendment (High Risk Terrorist Offenders) Act 2016 which introduced a framework into Part 5.3 of the Criminal Code for the continued detention of high risk terrorist offenders serving custodial sentences who are considered by a court to present an unacceptable risk to the community.

Towards the end of the decade the operation of anti-terrorism laws with sunset dates was extended by three years to 7 September 2021 by the Counter-Terrorism Legislation Amendment Bill (No. 1) 2018. This Act extended the operation of control order regime in Division 104 of the Criminal Code, the preventative detention order regime in Division 105 of the Criminal Code, the declared area provisions in sections 11ɔ.2 and 11ɔ.3 of the Criminal Code, and the stop, search and seizure powers in Division 3A of Part IAA of the Crimes Act 1914. In addition, new laws intended to combat terrorism focused on the perceived risk posed by radicalised Australians returning home.

The Crimes Legislation Amendment (Police Powers at Airports) Act 2019 received assent on 28 October 201ɔ. This Act enables police to direct the presentation of evidence of identity by persons at major airports. The

police are also given power to issue move-on and stop directions.

Two other terrorism related bills were prepared and introduced before the May 2019 election but have not been reintroduced at the time of writing. The Counter-Terrorism (Temporary Exclusion Orders) Bill 2019. The simplified outline describes the purpose of the bill as "The Minister may make an order (called a temporary exclusion order) that prevents a person from entering Australia for a specified period, which may be up to 2 years. An order cannot be made unless certain conditions are met, and it can be revoked."

3. The Decade Past: laws for surveillance, evidence gathering and agency powers

In May 2012 the Parliamentary Joint Committee on Intelligence and Security (PJCIS) was requested to conduct an inquiry into the reforms of Australian's National Security legislation. The PJCIS report was published on 24 June 2013 and the government responded on 1 July 2015. Many of the major changes to surveillance, evidence gathering and agency powers that took place in the remainder of decade came from or were related to recommendations by PJCIS in its report.

The Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 received assent on 13 April 2015 introducing a 2 year mandatory data a retention obligation for services "carrying communications, or enabling them to be carried" provided by carriers and carriage service providers. The data that must be retained includes user details, destination, date and time, and the type of service used. Being data rather than "content" this information is accessible to listed enforcement agencies and some state authorities with independent powers of access by issuing an authorisation. A warrant is not required. Importantly, an enforcement agency cannot issue an authorisation for access to metadata if the issuing party knows or reasonably believes the person to be working in the capacity of a journalist or is the employer of such a person and the purpose of the authorisation is to identify a source unless a journalist information warrant has been issued according to certain public interest criteria. According to the relevant Telecommunications (Interception and Access) Act 1979 (TIA Act) Annual Reports, 2 Journalist Information Warrants allowed 58 authorisations in 2017-18 and 6 allowed 20 authorisations in 2018-19. The data retention laws are subject to automatic review by the PJCIS. A review is currently underway and due to report 30 June 2020.

The Telecommunications and Other Legislation Amendment Act 2016 report 2017 received Assent on 18 September 2017 introducing national security related amendments to the Telecommunications Act 1997 (Telecoms Act). These amendments are known as the telecommunication security sector reforms or TSSR. The TSSR create an obligation on carriers and carriage service providers to "do their best" to:

> "...protect telecommunications networks and facilities owned, operated or used by the carrier or provider from or unauthorised interference or unauthorised access to ensure the:
>
> (c) confidentiality of communications carried on and of information contained on, communications networks or facilities; and
>
> (d) availability and integrity of communications networks and facilities."

The obligation extends to requiring a carrier or carriage service provider to notify the Department of Home Affairs if it proposes to make any change to its networks or facilities which may be adverse to security. Carriers and nominated carriage service providers can notify Home Affairs and receive an indication of whether or not Home Affairs has any concern. If there is an indication of concern and the carrier does not remediate as recommended by the department, the Minister has a broad power to negotiate or seek a security assessment from ASIO, which if adverse, allows the Minister to direct the regulated entity to comply (or take any other steps).

On 23 August 2018 the Minister issued "5G Security Guidance" to Australian carriers referencing the TSSR which included the statement "The Government considers that the involvement of vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law, may risk failure by the carrier to adequately protect a 5G network from unauthorised access or interference." With reference to this statement but, apparently without any other formal action by the government, TPG announced it would not use Huawei or TE equipment in its network.

The Security of Critical Infrastructure Act 2018 received assent on 11 April 2018. This Act introduced a scheme to improve the national security posture of specified ports, qualifying power generation gas supply and water facilities. The Minister has power to declare other infrastructure subject to the regime. The owners and operators are required to prepare and file with Home Affairs information regarding their identity (including their nationality) and the same information in relation to shareholders with a specified holding and all controlling entities. The information must be updated within 30 days of any substantive change. The Minister has the power to make directions regarding ownership or operation of the asset should the Minister obtain an adverse determination by ASIO that a matter notified is adverse to national security. This power could

be used to direct asset owners or operators to transfer their interest or to bring onshore or implement replacement technical solutions.

The Foreign Influence Transparency Scheme Act 2018 received assent on 29 June 2018. This regime requires a person acting on behalf of foreign government or political organisation to register with the Commonwealth. The Act does not require foreign entities who happen to be foreign owned or controlled to register and does not require registration by business contractors not engaged in communications, advocacy or lobbying. After the introduction of this scheme lobbyists, advocates and lawyers engaging in policy work must take care to establish the ownership and control of their clients.

National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018 received assent on 30 June 2018. This Act amended the Criminal Code to add new offences related to treason and espionage. The Act introduced offences for public servants acting against the Australian national interest and generally applicable offences of being reckless regarding Australian national security when dealing with certain information and certain foreigners. Responding to the potential impact of the new offences, a multinational university research project was formed and, in November 2019, Guidelines to Counter Foreign Interference in the Australian University Sector were published.

The Telecommunications and Other Legislation Amendment (Assistance and Access Act 2018 received assent on 8 December 2018. Also known as the "Encryption Act" this Act introduced a new Part 15 to the Telecoms Act and made significant amendments to the Surveillance Devices Act 2004 and the Australian Security Intelligence Organisation Act 1979 (amongst many others) directed at improving the effectiveness and agility of national security and law enforcement agencies. The new Part 15 introduces a new wide class of regulated entities called "designated communications providers" (DSPs). DSPs include carriers, carriage service provides and a wide range of electronic services, software, equipment and facilities providers involved with systems that carry communications. Listed agencies called "interception agencies" can request or require assistance from DSPs including removing one or more forms of electronic protection, providing technical information, installing, maintaining or testing the using of software and equipment as well as facilitating objectives of the relevant agency. This Act passed on the last day of Parliament in 2018 subject to an informal agreement between the government and the Labor Party that certain matters would be addressed. There is currently a Bill before parliament proposing a series of amendments and a government initiated a review conducted by the PJCIS which has been referred to the Independent Security Legislation Monitor (ISLM). The ISLM has been taking submissions and has indicated an intention to report by 30 June 2020.

Towards the end of the decade the government established the Home Affairs portfolio and increased the power of national security agencies including by passing the Home Affairs and Integrity Agencies Legislation Amendment Act 2018. Home Affairs is responsible for immigration, border protection, domestic security and law enforcement agencies. The Act also reformed the Attorney-General's oversight of Australia's intelligence community and agencies in the Home Affairs portfolio. There was also Intelligence Services Amendment Act 2018 which enables the Minister to protect persons outside Australia with an Australian Secret Intelligence Service (ASIS) member or agent and authorise the ASIS staff member to use "reasonable and necessary force" in the performance of his or her functions.

4. Changes on the Horizon

Use of facial recognition technology by government services is on the way. In October of 2019 the PJCIS issued an advisory report on the Identity-matching Services Bill 2019 (IMS) and the Australian Passports Amendment (Identity-matching Services) Bill 2019 (Passports Bill). The IMS seeks to establish services to identify, recognise or verify facial images and systems for collection, access, use, sharing and disclosure related data. The Department of Home Affairs would create and maintain facilities for the sharing of facial images and other identity information between government agencies, and in some cases, non-government entities. It will support a federated database of information contained in government identity documents such as driver licences.

Although expressing support for the rationale behind each bill, the PJCIS recommended that the IMS be redrafted to create a regime built "around privacy, transparency and subject to robust safeguards" to improve transparency, reporting and to clearly state the obligations of participating parties. The PJCIS also recommended that the Passports Bill be amended to ensure that automated decision making could only be used for decisions that produce favourable or neutral outcomes for the subject, and that such decisions would not negatively affect a person's legal rights or obligations, and would not generate a reason to seek review.

In a recent hearing on the Encryption Act, the ISLM gave an opening statement that indicated some thinking on changes to the Act. In particular, he appears in favour of some form of judicial supervision of requests and notices issued under Part 15 of the Telecoms Act including a review process that might publish reasons for decisions made in order to provide public guidance improved clarity of the limiting terms "systemic weakness" and "systemic vulnerability" by inclusion of statutory examples in the law. The views of the ISLM

suggest that some of the sought after improvements of the Encryption Act may eventuate.

On 7 October 2019, there was a joint statement issued by US Attorney General William Barr and the Minister for Home Affairs, Peter Dutton on the US Cloud Act. On 5 March 2020 the federal government introduced the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 in the House of Representatives. The proposed new law will allow Australian law enforcement and national security agencies to issue international production orders (IPOs) to communications service providers outside Australia in certain circumstances and facilitates compliance with IPOs from offshore by telecommunications providers in Australia.

5. Issues for the future

Without a crystal ball and not being a member of our national security apparatus the writer is not in a good position to predict what further controls and powers the Minister and our agencies might wish to legislate. I can however comment on some areas that clearly require careful attention:

- The distinction between metadata and content. The Attorney General responsible for introducing the mandatory data retention regime famously underplayed the power of metadata by comparing it to the information on the outside of an envelope. Under the existing regime national security and law enforcement bodies access up to 2 years of historical metadata and identify future metadata in real time without a warrant. It might be argued that some information about an electronic device is less privacy intrusive than some things a person might say while using the device. However, a real time feed of metadata from a person's device and/or 2 years of data indicating where they have been, who they called and how long they spoke to them, is not less privacy inclusive. It currently requires a warrant to place a tracking device on an individual's person or property but two years of metadata can be obtained on written request. The information content of metadata was highlighted in a recent answer by the Commonwealth Ombudsman, Michael Manthorpe, to a question raised in the PJCIS review of the mandatory data retention regime. Mr Manthorpe reported that metadata being supplied to agencies included the full URL being visited and therefore indicated content being viewed by the subject individual.
- The meaning of "communication". The Telecoms act defines the word "communication" inclusively to cover a conversation and a message whether in the form of sounds, data, text, visual images or signals. This definition does not sit well with the mandatory data retention regime or the TIA Act because it captures data and machine messages that should not be subject to regulation or storage and, in particular, may create unreasonable regulatory obligations for IoT networks
- Regulation of direct access to information systems. Our legislation presumes that agencies cannot obtain third party information except by request or compulsory acquisition. However, the Encryption Act now gives interception agencies the power to install or have built their own direct access to third party information. If such a point of access was constructed, the agency would not have to require data by warrant or authorisation, it could be collected or delivered by the technology of the agency. s317 H (1) to the Telecoms Act attempts to address this issue by expressly maintaining existing requirements to use a warrant or authorisation to obtain data but considering the step change in agency power introduced by the Encryption Act (i.e. the ability to install software or equipment on a third party system without a warrant) it may be unnecessary to request data from a designated communication provider at all. The Encryption Act appears to open a major gap in the information security framework.
- The role and regulation of surveillance. The TIA Act authorises the disclosure of prospective telecommunication data. According to the latest report on the TIA Act for 2018-2019, 27,824 authorisations for prospective data were issued during the period of the report. The writer understands that when prospective data is requested, it may be provided in real time. If the data provided includes information in the mandatory data retention data set (which would seem likely) the provision of prospective information clearly amounts to real-time surveillance of the location and calling activity the subject of the authorisation. The powers in the Encryption Act could be used to obtain a similar feed of real time information from over-the-top service providers. Considering that the Australian Securities and Investment Commission currently monitors the trading on the Australian Stock Exchange in real time for insider trading using a data analytics engine, we might reasonably expect our national security and law enforcement agencies to seek to review "prospective data" in bulk to look for patterns and behaviours that indicates unlawful activity. Considering such data could be obtained with a single prospective authorisation issued on the agency's own initiative, this may be happening already.

- Protection of a free press. The journalist information warrant regime in the TIA Act does not prevent the use of metadata to identify a journalist's source unless the authorisation pertains to the data of a journalist or his or her employer. In addition, the journalist warrant regime does not moderate the other various criminal offences that prevent publication of information about national security activities and operations even when to do so would be in the public interest. A discussion paper by The Alliance for Journalists' Freedom advocates a Media Freedom Act aimed at "striking the right balance in National Security Legislation". Calls for moderation of national security laws to protect journalists and a free press are likely to persist.
- Adverse impacts on industry. Two examples:
    - Encryption and security tool developers in Australia expressed alarm regarding the Encryption Act because the law gives interception agencies the ability to access, copy and amend the source code of their products making them potentially undesirable. At one industry forum, the CEO of a leading software company said that he was being forced to move all development offshore.
    - The mandatory data retention regime imposes an onerous retention obligation on any communication service provider that happens to resell carriage. This creates a strong incentive for system integrators and data centre providers to avoid selling carriage to their customers even when it would be profitable to do so. The adverse impact of the existing regimes on Australian industry is likely to remain a basis for reform of these regimes in the coming decade.

More broadly, during consultations on Australia's 2020 Cyber Security Strategy it has been suggested that key strategic information systems should be hardened by a new TSSR type system protection obligations or the imposition of standards or a code.

6. Conclusion

Our national security laws have been changing rapidly in a rapidly changing environment. With this in mind, it is neither surprising that many aspects of the regime have raised serious issues nor that many aspects are subject to ongoing review and have further significant changes on the horizon.

Patrick Fair is the principal of Patrick Fair Associates, an Adjunct Professor at the School of Information Technology, Faculty of Science, Engineering and Built Environment at Deakin University, the Chairman of the Communications Security Reference Panel at the Communications Alliance, and General Advisor for LexisNexis Practical Guidance Cybersecurity, Data Protection and Privacy.