SAFE AND FREE:
NATIONAL SECURITY SURVEILLANCE AND THE RULE OF LAW ACROSS DEMOCRATIC STATES

The University of Texas at Austin
Strauss CENTER
for International Security and Law

UNDERSTANDING AUSTRALIA'S APPROACH TO ELECTRONIC SURVEILLANCE

William A. Stoltz

ABOUT THE AUTHOR

Dr. William A. Stoltz is a Senior Fellow at the Australian National University's National Security College and a Senior Manager at Cyber CX, Australia's leading cyber security firm. He has previously worked across Australia's defence, intelligence, and law enforcement communities developing strategic policy, legislative reform, and strategic intelligence assessments. He writes extensively on national security and intelligence policy reform as well as Australian foreign policy.

Stoltz is a Visiting Fellow at the Robert Menzies Institute at the University of Melbourne and an Associate Member of the Centre for the Study of Subversion, Unconventional Interventions and Terrorism (SUIT) at the University of Nottingham.

He holds a PhD and Advanced Masters of National Security Policy from the Australian National University as well as a Bachelor of Arts from the University of Melbourne.

ACKNOWLEDGEMENTS

This project was supported by funds from the Robert Strauss Endowment at the University of Texas at Austin and by a charitable gift from Microsoft. Each paper in the Safe and Free series reflects the views of its author. Editorial direction for the series was provided by Adam Klein, Director of the Robert Strauss Center for International Security and Law at the University of Texas at Austin. We are grateful to Strauss Center staff members Ali Prince and Brittany Horton, and to associate editors Zachary Badore, Seth Greenwald, and Taylor Helmcamp, for their help in shepherding the Safe and Free series to publication.

CONTENTS

NOVEMBER 2023

I. INTRODUCTION

Surveillance has always been one of the fundamental tasks of any intelligence organisation. Exercised correctly, it can yield vital insights into the pattern of life and motivations of individuals as well as the strengths and weaknesses of entire organisations, including criminal gangs, terrorist cells, even entire governments. For intelligence and law enforcement investigations alike, it is a critical practice. In the digital age, electronic surveillance has arguably displaced physical surveillance activities as the 'bread and butter' of these investigations. Certainly, in the Australian context necessity has seen the Commonwealth government extend electronic surveillance powers to a wide range of agencies who exercise them in relation to every conceivable variety of criminal or national security target.

However, despite the frequency with which electronic surveillance is used, and the wide range of targets it affects, Australia's is arguably one of the most stringent electronic surveillance regimes in the world. As this piece outlines, the practice of electronic surveillance is tightly bound to strict contextual limitations and requirements. Different agencies are given distinct legislated remits in which to work, restricting whether or not they can surveil Australians or foreigners, whether they can collect evidence or intelligence, and whether they require the authorisation of judicial officers or a Commonwealth minister.

Australian agencies are also subject to a robust and multilayered oversight and accountability ecosystem which uses internal contestability, ministerial authorisations, parliamentary review, and independent scrutiny to create a compliance culture that is highly non-permissive to the abuse or maladministration of agencies' extraordinary powers. Australia's highly regulated regime is dynamic and has been shaped by a near constant process of trial and adjustment that calibrates and refines agencies' powers to match new technologies, shifting threats, and evolving community expectations. Indeed, the technological disruption of the modern investigative operating environment has resulted in a comprehensive rewriting of Australia's electronic surveillance legislation that is currently underway and expected to be implemented over the course of the next two years.

II. INSTITUTIONS

Operational Entities

The operational use of electronic surveillance in Australia spans multiple jurisdictions and purposes.

The Australian Security Intelligence Organisation (ASIO), Australia's primary domestic intelligence agency, conducts electronic surveillance for the purpose of collecting intelligence on malicious actors operating against Australia's interests. This has typically comprised various terrorist organisations, subversive political groups, and dangerous fixated individuals. However, in recent times ASIO's primary target has been foreign intelligence services and their affiliates operating in Australia, namely those operating on behalf of the People's Republic of China (PRC). ASIO's electronic surveillance powers are established in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act). Before conducting electronic surveillance, ASIO obtains surveillance device warrants approved by the Attorney-General upon the recommendation of the Director-General of Security, a civil servant also appointed under the ASIO Act.[1]

The Australian Signals Directorate (ASD) is Australia's primary agency for communications intelligence or COMINT and other types of signals intelligence, or SIGINT, with a focus on foreign intelligence targets. It is also responsible for offensive cyber operations. ASD therefore conducts various forms of electronic surveillance in service of its foreign intelligence collection and covert action functions. ASD's priority is to support the Australian Defence Force as well as its counterpart agencies in the National Intelligence Community (NIC).[2] The targeting of Australians as part of ASD's foreign intelligence remit is tightly restricted and subject to ministerial authorisation.[3] While ASD may not initiate intelligence collection, including electronic surveillance, on domestic targets, including Australians within Australia, ASD is able to provide technical support to Australian agencies with domestic intelligence and law enforcement remits. This in effect means that at the request of domestic agencies ASD is able to exercise its digital capabilities within Australia to perform electronic surveillance for the operational benefit of those domestic agencies.

The Australian Secret Intelligence Service (ASIS) has a special remit to collect foreign intelligence, namely human intelligence or HUMINT, and undertake covert actions abroad.[4] ASIS undertakes electronic surveillance in support of its HUMINT targeting and typically as part of joint operations with ASIO and/or ASD; with the later agency likely responsible for the more technically complex instances of electronic surveillance. This joint operating model is demonstrative of the fusion of HUMINT and SIGINT, which is sometimes referred to as signals-enabled human intelligence or human-enabled signals intelligence, as the case may be.

> ***The exercise of the AFP's electronic surveillance powers is largely for the purposes of evidence collection, however in recent years it has acquired additional powers that allow it to undertake electronic surveillance for the purpose of collecting criminal intelligence.***

Australia's national law enforcement agency is the Australian Federal Police (AFP), which is responsible for enforcing Commonwealth legislation and assisting State and Territory law enforcement agencies. Aside from the use of electronic surveillance powers for the purposes of conventional law enforcement, the AFP undertakes electronic surveillance to investigate and prosecute national security offences, typically in concert with ASIO. In recent times, the national security investigations which have most occupied the AFP have been for terrorism offences, foreign interference offences, and offences concerning transnational serious and organised crime (TSOC), which the Australian government regards as a national security threat.[5] The exercise of the AFP's electronic surveillance powers is largely for the purposes of evidence collection, however in recent years it has acquired additional powers that allow it to undertake electronic surveillance for the purpose of collecting criminal intelligence. Operationally, the AFP is closely assisted by ASIO and ASD in carrying out electronic surveillance. In relation to cyber threats, the AFP jointly operates with ASIO, ASD and other Commonwealth, State and Territory agencies via the Australian Cyber Security Centre, a body in which agencies co-locate staff to undertake law enforcement and intelligence

operations in concert.[6]

The Australian Criminal Intelligence Commission (ACIC) is the Commonwealth's peak criminal intelligence body with extraordinary powers for disrupting, investigating and collecting intelligence in relation to the most pernicious criminal threats to Australia's security.[7] It operates within Australia and abroad. Transnational criminal groups operating against Australia are the main concern for the ACIC, including drug syndicates, people smugglers, money launderers, firearms traffickers, and cybercriminals. The ACIC is able to undertake electronic surveillance against these targets for the purposes of collecting evidence and intelligence. Alongside the Australian Federal Police, the ACIC has recently been empowered to undertake electronic surveillance in relation to entire malicious networks, not just individuals.[8] It has also been given powers that will allow the ACIC to use electronic surveillance information for the purpose of undertaking 'data disruption' operations (aka offensive cyber operations) against particular criminal targets.[9]

Alongside the AFP and the ACIC, there are a number of State and Territory law enforcement agencies that undertake electronic surveillance within their respective jurisdictions against national security targets, namely terrorist and transnational criminal groups. These agencies include conventional police forces as well as crime commissions which have special powers for collecting criminal intelligence primarily for the purpose of addressing transnational organized crime. These domestic law enforcement agencies operate closely with the AFP and ACIC and can receive technical support from ASD to undertake especially complex electronic surveillance activities against national security targets. As this paper is primarily concerned with electronic surveillance undertaken for national security purposes, it will focus predominantly on the Commonwealth (aka the federal) jurisdiction.

Authorising Entities

Electronic surveillance activities by Australian's foreign intelligence agencies, ASD and ASIS, are authorised as part of approvals given for a wider operation. Where operations relate to the collection of intelligence on an Australian, a combination of consultation and approval from the Foreign Minister, Defence Minister, and Attorney-General is typically required.[10] Lower risk operations, including those not relating to Australian targets, can be approved by the directors general of ASD and ASIS, or their delegates. Like the head of ASIO, the directors general of ASD and ASIS are statutory appointments empowered under by the *Intelligence Services Act, 2001* (IS Act).

Operations that are presented to ministers for approval will have typically been developed with the input of relevant policy departments. For example, where ASIS may wish to undertake an intelligence operation involving an overseas target it will have consulted closely with officials in the Department of Foreign Affairs and Trade about the potential effect on the relevant country before presenting the operation for the approval of the Foreign Minister. Information about the ASD and ASIS operations approved or not approved is selectively disclosed by agency heads to the Parliament via the Parliamentary Joint Committee on Intelligence and Security (PJCIS), but is not made public. Indeed, even information regarding historical operations typically remains classified and withheld by the National Archives of Australia.

Aside from the foreign intelligence agencies of ASD and ASIS, the main means by which electronic surveillance activities are approved in the Australian system is via the authorisation of warrants. These fall into two general categories: warrants authorised by a judicial official and warrants authorised by a minister. ASIO's surveillance activities are approved via warrants issued by the Attorney-General. The AFP, ACIC, and State and Territory agencies undertake electronic surveillance activities using warrants authorised by a relevant judge or nominated member of the Administrative Appeals Tribunal.[11]

For Commonwealth agencies (i.e., agencies of the national government), all electronic surveillance powers are provided for in laws laid down by the Parliament, which are subject to periodic review as well as sun-setting provisions in some cases. State and Territory legislatures similarly provide for electronic surveillance powers in their jurisdictions. However, no Australian parliament has a role in authorising operations, including those in which electronic surveillance may occur.

Oversight Entities

There are, broadly speaking, two forms of oversight in the Australian system relevant to the use of electronic surveillance: operational oversight and legislative oversight.

What we might describe as operational oversight includes those agencies and internal agency offices that are responsible for evaluating whether individual instances of electronic surveillance have been operationally effective, lawful, and proportionate to the offence or threat being investigated. This also includes evaluation concerning whether electronic surveillance information is being appropriately stored, disseminated, and destroyed.

What we might describe as operational oversight includes those agencies and internal agency offices that are responsible for evaluating whether individual instances of electronic surveillance have been operationally effective, lawful, and proportionate to the offence or threat being investigated.

The first rank of entities responsible for this kind of oversight are the internal assurance and compliance units within each of the operational agencies themselves. These internal agency units can be directly involved in the planning and alteration of active investigations or operations. These units will audit the teams undertaking surveillance and scrutinise the work of individual surveillance officers to ensure that their investigations match the authorisations provided. Internal assurance and compliance units are often overlooked when discussing oversight because they are not strictly statutory bodies so don't have special oversight powers per se. However, they are essential to inculcating a strong compliance culture within agencies and are arguably the first line of defence against the misuse of surveillance powers.

The next level of operational oversight at the Commonwealth level is conducted by several standalone oversight agencies: the Commonwealth Ombudsman, the Inspector General of Intelligence and Security, and the Australian Commission for Law Enforcement Integrity, all of which typically play a post-facto role.

- The Commonwealth Ombudsman. The Commonwealth Ombudsman has a broad responsibility for providing assurance to the government regarding the public administration of Commonwealth entities. In this capacity it has an ongoing role in evaluating the activities and administration of the AFP and the ACIC in particular. For law enforcement agencies, Parliament has regularly included mandatory reporting to the Ombudsman in electronic surveillance legislation as a means to establish regular and independent review of how agencies are using these powers.

- The Inspector General of Intelligence and Security (IGIS). The IGIS has a remit to examine the lawfulness and probity of all activities undertaken by what is typically referred to as the Australian Intelligence Community (AIC)[12] as well as partial oversight for the intelligence functions of the AFP and the ACIC. This means that the IGIS can evaluate not just whether agencies' use of their powers has been strictly lawful, but whether this use has been undertaken in a proportionate and ethical manner subject to rigorous internal contestability and scrutiny. In this way the IGIS oversees the integrity as well as the efficacy of operations. The IGIS is equipped with expansive powers to access and investigate the facilities and information of agencies. Its investigations can be self-initiated or commenced based on referrals, including from the general public, as well as complaints by individual officials within relevant agencies. In relation to electronic surveillance, the IGIS will examine not only the collection of intelligence but also its storage, dissemination and disposal. It is the most powerful and most important of Australia's intelligence oversight institutions.

- The Australian Commission for Law Enforcement Integrity handles integrity investigations, such as looking at instances of alleged corruption or inappropriate conduct by law enforcement personnel. In this way ACLEI's investigations can interact with wider operational oversight by investigating the conduct of individuals officials in the context of operations. Bodies under its remit include the ACIC, AFP, the Department of Home Affairs, the Australian

Border Force (ABF), and the Australian Transaction Reports and Analysis Centre (AUSTRAC).[13]

Legislative oversight encompasses those entities that can evaluate the effectiveness and proportionality of the enabling legislation that makes electronic surveillance by the state lawful. These entities mainly include those of the Parliament of Australia, but also includes a number of organisations separate from the legislature. Broadly speaking, Parliament exercises its oversight of the national security and law enforcement legislation that enables electronic surveillance via parliamentary committees. There are three types of committees: House of Representatives committees, Senate committees, and joint committees comprising members from both houses of parliament. Unlike House of Representatives committees and joint committees, Senate committees are not always established at the behest of the government-of-the-day because historically speaking the government rarely commands a majority in the Senate. Of the myriad committees that can conceivably interact with electronic surveillance, the following two are the most powerful.

- The Parliamentary Joint Committee on Intelligence and Security (PJCIS) is the only Parliamentary committee that is mandated by law to exist and provides its members with special, additional rights and responsibilities.[14] The PJCIS is primarily responsible for undertaking inquiries concerning the NIC agencies, such as new proposed legislation, and matters of national security; these inquiries are typically referred to it by the government, but it can also initiate its own inquires. It is in this capacity that the PJCIS often interacts with questions relating to electronic surveillance. There are also a number of instances in which the PJCIS requires agencies to report to the Committee on the use of its powers as well as cases where so-called 'sun-setting' clauses require the Committee to re-evaluate legislated powers and make a recommendation to the Parliament as to whether they should be retained. This includes some electronic surveillance powers provided to the AFP and ACIC in the *Surveillance Devices Act 2004* (SD Act).[15]

- The Parliamentary Joint Committee on Law Enforcement (PJCLE) is comparatively less powerful than the PJCIS and focuses exclusively on law enforcement powers. However, in the case of electronic surveillance carried out by law enforcement agencies and laws affecting this surveillance, the PJCLE has a regular role in reviewing legislation.

There are other institutions of note outside of parliament that exercise a degree of legislative oversight.

- The Independent National Security Legislation Monitor (INSLM). The INSLM is a statutory appointment typically held by a former judge. The INSLM regularly reviews extant national security legislation and proposed bills to evaluate their effectiveness, probity, and proportionality. It can initiate its own reviews, can be asked by Parliament (typically via the PJCIS) to review legislation and in some cases is mandated to review certain laws at set intervals. The INSLM has recently considered electronic surveillance legislation in its review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018*.[16] The INSLM's recommendations are non-binding and can remain classified. Nevertheless, the INSLM is a critical source of external expert advice to Parliament and the government on complex pieces of national security law.

- Royal Commissions. Traditional judicial oversight—i.e., rulings by judges—of Australian national security laws, including electronic surveillance laws, is rare. This is because relevant courts up to and including the High Court can only consider such legislation in the context of a case put before it. Historically however, some of the most seminal decisions regarding Australian

national security law have been laid down by Royal Commissions—special independent inquires instigated by the government, typically overseen by a senior judge and empowered with extraordinary powers of inquiry including the ability to compel the production of evidence, the appearance of witnesses, and the carrying out of classified hearings.

The most important Royal Commissions in this regard have been the two Royal Commissions into Intelligence and Security conducted by Justice Robert Marsden Hope in 1974 and 1984, respectively.[17] The Hope Royal Commissions evaluated the need for a Commonwealth system of security and intelligence agencies; the ideal governance for such a system; as well as the efficacy with which extant agencies had been performing their functions. The Commissions therefore laid down many of the principles that would be reflected in subsequent national security legislation, including those laws governing electronic surveillance. Some of those principles include those already mentioned, such as the need for parliamentary oversight, the use of warrants, and the separation of domestic and foreign intelligence collection activities.

- Independent reviews. Separate from Royal Commissions, there have been a number of independent reviews commissioned by the government of the day. These independent reviews have not historically been given special powers, and their remit and resourcing has varied. They have provided the basis for incremental reform and modernisation of Australia's intelligence system based on expert advice, typically external from the civil service. Some relevant examples include:

  - The 1995 Commission of Inquiry into the Australian Secret Intelligence Service by Gordan Samuels (the Samuels Inquiry), which evaluated the performance and oversight of ASIS following a number of high-profile accusations of malpractice.[18]
  - The 2004 Inquiry into Australian Intelligence Agencies by Philip Flood (the Flood Inquiry), which evaluated the performance of Australia's intelligence assessment infrastructure following the 2003 invasion of Iraq and Australia's initiation of its Regional Assistance Mission to the Solomon Islands (RAMSI).[19]
  - The 2017 Independent Intelligence Review by Michael L'Estrange and Stephen Merchant (the L'Estrange Review), which assessed the overall structure of Australia's intelligence community and recommended the creation of a new National Intelligence Community apparatus for managing oversight and joint capability investment.[20]
  - The 2020 Comprehensive review of the legal framework of the National Intelligence Community by Dennis Richardson (the Richardson Review) which scrutinised the contemporary effectiveness and long-term suitability of Australia's intelligence legislation.[21]

III. OPERATIONAL CAPABILITIES AND PRIORITIES

Australia's agencies maintain a great deal of secrecy around the nature of their intelligence collection capabilities and operational methodologies generally, and their electronic surveillance capabilities are no exception. So, it is difficult to speak definitively about the sophistication of Australia's capabilities given the paucity of publicly available information. Indeed, it has been suggested that of the Five Eyes nations, Australia is the least open about its intelligence capabilities.[22]

For example, the Australian government only acknowledged in 2017 that its peak cyber security agency—the Australian Signals Directorate—exercised offensive cyber capabilities, well after its Five Eyes counterparts had long since avowed their own offensive cyber roles.[23] Confined then to open source material, we can only evaluate the relative sophistication of Australia's capabilities for electronic surveillance via broad inferences. To this end, there are three data points we can observe that the reader may find constructive in understanding Australia's electronic surveillance capabilities: agencies' legislated powers, publicly known operations, and agencies' relationships with private telecommunications firms which support the conduct of electronic surveillance.

We will discuss relevant legislation in more detail later, but it can be said that Australia's Parliament has provided the legal framework for agencies to build and operationalise a robust and technologically sophisticated system for undertaking electronic surveillance against diverse and hardened targets. We know that in the face of an increasingly less permissive digital operating environment successive governments have maintained high expectations that agencies will be able to successfully respond to myriad malicious actors, including terrorist groups, organised criminals, child exploitation rings, and agents of foreign governments.[24]

Agencies' funding would suggest that the Australian government intends for them to have the resources available to realise the fullest operational impact for which the law provides. For example, recent legislative amendments have expanded the electronic surveillance powers of the AFP and ACIC to not only undertake electronic surveillance against a specific individual, but also to undertake simultaneous collection relating to an entire digital network, as well as to pivot from passive collection to offensive cyber operations.[25] The expedited passage of these amendments would tend to suggest an operational readiness—and therefore a capability—to exercise them.

Having said that, relevant legislation is also a window into the limitations of Australian capabilities. As alluded to earlier, the IS Act provides for ASD to give technical support to Commonwealth, State, and Territory agencies to assist them in carrying out their responsibilities and exercising their powers. Data is not available on how frequently this technical assistance provision is called upon, but its existence—ASD became subject to the IS Act in 2018—reflects a practical, cross-government need for support from Australia's primary digital intelligence agency.

...it can be said that Australia's Parliament has provided the legal framework for agencies to build and operationalise a robust and technologically sophisticated system for undertaking electronic surveillance against diverse and hardened targets.

Another indication of the capabilities available to Australian agencies is the nature of their relationship with private firms, namely the collaborative operational arrangements agencies have with telecommunications providers and digital firms. As the main carriage service providers in Australia, collaboration with Telstra, Optus, and Vodaphone is essential for agencies' exercise of electronic surveillance both for the purpose of collecting evidence and intelligence.[26] The T*elecommunications and Other Legislation Amendments (Assistance and Access) Act 2018* (the TOLA Act) provides a critical regime for agencies to leverage private firms' in-house technical capabilities for law enforcement and intelligence purposes.

The TOLA regime provides for three types of engagement: technical assistance requests, technical

assistance notices, and technical capability notices. As the name suggests, the technical assistance requests provide an avenue for telecommunications firms ("telcos") to assist intelligence and law enforcement agencies on a voluntary, negotiated basis while maintaining legal indemnity. Technical assistance notices by comparison compel telcos to leverage existing systems to support agencies, while technical capability notices go further still by compelling telcos to build a new technical capability for the purpose of supporting agencies.

Mechanisms such as the TOLA regime stand alongside myriad commercial arrangements agencies have with private firms to support electronic surveillance capabilities. Some critics perceive these arrangements as a troubling marriage of state security and surveillance capitalism,[27] while others counter that these are essential partnerships to avoid the problem of 'going dark' that advances in digital communications present to investigators.[28]

The relationship Australia's law enforcement and intelligence agencies have with private firms, particularly telcos, suggests on the one hand that agencies' in-house capabilities are not sufficient to keep-up with the scale and complexity of the modern task of electronic surveillance. On the other hand, however, this seeming reliance on non-government firms speaks to the sophisticated digital surveillance tools that reside in the private sector, which when taken in aggregate with government capabilities likely makes Australia's capacity for electronic surveillance formidable.

Intelligence Priorities

Australia's exercise of electronic surveillance for intelligence collection is subject to the Commonwealth's overarching process for directing intelligence collection. Australia's Prime Minister, typically following consultation with relevant Cabinet ministers, approves Australia's National Intelligence Priorities (NIPs) for the National Intelligence Community (NIC). The Director-General of National Intelligence, and the Office of National Intelligence (ONI) they lead, is responsible for advising the Prime Minister on the NIPs and ensuring the NIC is resourced and calibrated accordingly.

It is understood that these classified NIPs are not necessarily updated on a mandated or fixed annual basis, but rather are updated following evaluation and advice from ONI following changes to the government's policy agenda and/or shifts in the strategic environment. To ensure the NIC is appropriately serving the government's NIPs, ONI helps agencies to identify a set of intelligence missions: general targets for collection and analysis that the NIC agencies need to focus on in order to service the government's NIPs.

IV. RELEVANT LAW AND TRANSPARENCY

Australia's electronic surveillance regime is highly codified by a suite of legislation that has been laid down over the past fifty years and routinely refined by Australia's Parliament. Despite the statutorily constrained nature of Australia's framework, agencies' use of electronic surveillance is still somewhat opaque. For law enforcement agencies, annual reporting provides the overall numbers of authorisations that are approved or refused, but little insight is given into the typical basis for refusal or key factors driving approval.[29] For intelligence agencies, even the numbers of authorisations are hard to discern, let alone more contextual information that might help Australians understand the typical nature of the targets or the urgency with which surveillance is undertaken.

Prior to the *Australian Security Intelligence Organisation Act of 1956*, none of the powers of an Australian intelligence agency had been defined in law, and it would not be until the *Intelligence Services Act of 2001* that all of Australia's intelligence agencies became statutory. Commonwealth law enforcement agencies by comparison had always had their role defined by Parliament.

Despite the modern reliance on codification to provide for the extent and limitations of agency powers, Australia has no explicit constitutional protections for privacy or free speech, nor any provisions directly relating to surveillance. Instead, in Australia's Westminster tradition of jurisprudence, Australia operates under *implied* rights to free speech, privacy, and other civil liberties that have been affirmed by Australia's High Court. For example, Australians have an implied constitutional right to free speech because while the constitution does not explicitly mention citizens' free speech rights, it does specify direct elections for which free speech is an essential enabler.

Despite past uses of executive power alone, today the exercise of electronic surveillance by Australian intelligence and law enforcement agencies is provided for by a number of Acts of Parliament. These are the *Telecommunications Act 1997* (Telco Act), the *Australian Security Intelligence Organisation Act 1979* (ASIO Act), the *Surveillance Devices Act 2004* (SD Act), and the *Telecommunications (Interception and Access) Act 1979* (TIA Act). While the details of these acts are open, internal procedures and guidance, including the substance of legal interpretations pertaining to their use, is typically not publicly available. Details regarding how agency heads deliberate on the exercise of the powers delegated to them are also opaque.

> ***Prior to the Australian Security Intelligence Organisation Act of 1956, none of the powers of an Australian intelligence agency had been defined in law, and it would not be until the Intelligence Services Act of 2001 that all of Australia's intelligence agencies became statutory.***

The *Telecommunications Act 1997* (Telco Act) places restrictions and obligations on telecommunications companies with regards to the use and protection of electronic data. For example, it creates offences relating to the unauthorised use or disclosure of communications information whilst also providing 'carve outs' for permitted commercial and government purposes. The Telco Act creates a framework for industry assistance to intelligence and law enforcement agencies—the TOLA regime mentioned earlier. The Telco Act also mandates agencies to notify the IGIS and Commonwealth Ombudsman after using their industry assistance powers.

The *Australian Security Intelligence Organisation Act 1979* (ASIO Act) establishes ASIO's powers to undertake surveillance activities that would otherwise be an offence under the *Criminal Code Act 1995*. It does this by providing surveillance device warrants and computer access warrants, both of which can be approved by the Director-General of Security. The ASIO Act places a range of mandatory obligations on ASIO with regards to reporting the use of these powers to the relevant minister, the Parliament, and the IGIS.

The *Surveillance Devices Act 2004* (SD Act) creates the framework for the Australian Federal Police, the Australian Criminal Intelligence Commission, and the Australian Commission for Law Enforcement Integrity

to undertake electronic surveillance by providing for a series of relevant warrants. These warrants include surveillance device warrants, computer access warrants, network activity warrants, and data disruption warrants. To clarify the usage of these various warrants, the SD Act also provides definitions of key concepts such as the meaning of 'surveillance device' and what constitutes a computer.

The *Telecommunications (Interception and Access) Act 1979* (TIA Act) outlines how law enforcement and intelligence agencies should go about intercepting electronic communications and accessing stored communications data by allowing agencies to apply to use interception warrants and stored communications warrants. For law enforcement agencies, the TIA Act also specifies the severity of crime against which these warrants can be used, mandating that interception warrants can only be used to help investigations into offences attracting imprisonment of seven years or more. Similarly, stored communications warrants can only be used in response to offences attracting penalties of three years or more.

V. REFORMS AND OTHER IMPORTANT FACTORS

Australia is currently undertaking an initiative known simply as Electronic Surveillance Reform or ESR. The ESR initiative seeks to replace Australia's legacy electronic surveillance legislative regime—which currently spans multiple acts—with a single consolidated piece of legislation. This is to achieve a modernised, simpler legislative basis for electronic surveillance that is better suited to the current technology environment, easier for agencies to use, and easier to navigate for the purposes of oversight.

The ESR initiative represents the most complex piece of national security law reform in Australia in forty years.[30] The Australian government has undertaken an extensive public engagement program to explain the ESR initiative and garner community feedback. This is in response to past controversies that have surrounded the introduction of new national security powers for the digital age. The TOLA regime mentioned earlier attracted particular controversy when it was introduced in 2018 due to concerns from some civil society groups that it would facilitate mass surveillance and the circumvention of encryption to the detriment of journalists and whistle-blowers.[31]

In addition to the historic ESR legislative reform, over the next decade the Australian Signals Directorate will be the recipient of the largest single investment in Australia's cyber and intelligence capabilities in the form of project REDSPICE, valued at approximately $10 billion (AUD). The project will, according to the government, bolster ASD's ranks by 1,900 additional personnel with the objective of tripling ASD's offensive cyber capability and improving its adoption of new advanced technologies, namely artificial intelligence and machine learning. This investment is being made, in part, due to the central role ASD now plays in supporting the electronic surveillance activities of agencies across Australia as well as its own surveillance operations.[32]

Alongside these structural reforms, Australia's national security operating environment has changed markedly since approximately 2016, when Australia's relationship with the People's Republic of China (PRC) begun to acutely deteriorate. In response to a number of high-profile instances of attempted foreign interference, including some involving Australian politicians,[33] the Australian government introduced new foreign interference laws and ASIO begun to engage more openly with the Australian public about the risk of foreign espionage and interference.[34] The Office of National Intelligence also deepened its engagement with the Australian business community in an effort to raise awareness of the risks to sensitive industries, especially concern foreign investment from PRC state-owned enterprises.[35]

> ***This operating model of using otherwise non-state criminal organisations to undertake state-directed covert action challenges traditional structures and conventions surrounding how Australian agencies exercise their powers; namely it muddles the traditional distinction that criminal actors will be treated as law enforcement targets while malicious state actors will be treated as national security targets.***

These tensions resulted in the PRC placing arbitrary sanctions on a range of Australian goods and breaking of most official-level engagement.[36] Since this time, ASIO has routinely identified foreign interference and espionage as its "primary security concern."[37] Increased public engagement from the likes of ASIO and ONI in response to the PRC's belligerence towards Australia has led to a marked shift in Australian public opinion towards China, with one poll indicating that 75% of Australians now regard the PRC as a threat to Australia, compared with 40% a decade earlier.[38] This shift in public mood has doubtless led to greater tolerance for the exercise of agency powers against agents of foreign interference.

However, the most important effect on the operating environment stemming from the PRC's targeting of Australia arises from the PRC's multi-modal approach to interference operations. Particularly in the cyber domain, the PRC has demonstrated a predilection for mobilising both official and non-official but state-

sponsored actors, including criminal organisations, to disrupt targets. In 2021 for example, the PRC sponsored a number of cybercrime groups to undertake a coordinated attack on the Microsoft Exchange servers, exposing the data of Microsoft clients worldwide.[39]

This operating model of using otherwise non-state criminal organisations to undertake state-directed covert action challenges traditional structures and conventions surrounding how Australian agencies exercise their powers; namely it muddles the traditional distinction that criminal actors will be treated as law enforcement targets while malicious state actors will be treated as national security targets. When it comes to the exercise of electronic surveillance and other investigative powers, this environment of intersecting threats has heightened the demand for intelligence and law enforcement agencies to jointly operate and coordinate their investigations like never before.

ENDNOTES

1. Mike Burgess, 'Director-General's Annual Threat Assessment | ASIO', February 2022, https://www.asio.gov.au/resources/speeches-and-statements/director-generals-annual-threat-assessment-2022.
2. Australian Signals Directorate, 'Who We Work With | Australian Signals Directorate', accessed 19 September 2022, https://www.asd.gov.au/about/who-we-work.
3. '*Intelligence Services Act 2001*' (Commonwealth of Australia, 2001), Section 7, http://www.legislation.gov.au/Details/C2022C00153.
4. Ibid
5. Commonwealth of Australia, 'National Strategy to Fight Transnational, Serious and Organised Crime', 2018.
6. Australian Cyber Security Centre, 'About the ACSC', cyber.gov.au, accessed 19 September 2022, https://www.cyber.gov.au/acsc..
7. Commonwealth of Australia, '*Australian Crime Commission Act 2002*' (Attorney-General's Department, 2002), https://www.legislation.gov.au/Details/C2022C001.
8. Commonwealth of Australia, '*Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*' (Attorney-General's Department, 2021), https://www.legislation.gov.au/Details/C2021A00098/Html/Text, http://www.legislation.gov.au/Details/C2021A00098.
9. Ibid.
10. '*Intelligence Services Act 2001*' Section 8.
11. Commonwealth of Australia, '*Surveillance Devices Act 2004*', Section 14, 2004, http://www.legislation.gov.au/Details/C2022C00180.
12. The Australian Intelligence Community is a shorthand reference for the 'traditional' intelligence agencies: the Office of National Intelligence, ASD, ASIS, ASIO, the Defence Intelligence Organisation, and the Australian Geospatial Organisation.
13. AUSTRAC is Australia's financial intelligence agency, specialising in countering financial crime, disrupting criminal financing, and investigating terrorism financing.
14. All other committees are dissolved when an iteration of parliament ends and are only reconstituted in the next parliament at the pleasure of the government but in the case of the PJCIS, the IS Act compels the government to recreate the PJCIS each time.
15. Commonwealth of Australia, '*Surveillance Devices Act 2004*' Section 27KAA.
16. Independent National Security Legislation Monitor, 'Review of *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* and Related Matters', 9 July 2020, https://www.inslm.gov.au/reviews-reports/telecommunications-and-other-legislation-amendment-act-2018-related-matters.
17. National Archives of Australia, 'Royal Commission on Intelligence and Security, 1974–77', History of Australian intelligence and security, accessed 19 September 2022, https://www.naa.gov.au/explore-collection/intelligence-and-security/history-australian-intelligence-and-security/royal-commission-intelligence-and-security-1974-77; Royal Commission on Australia's Security and Intelligence Agencies and Robert Marsden Hope, eds., *General Report*, Parliamentary Paper, no. 231 of 1985 (Canberra: Australian Government Publishing Service, 1985), https://nla.gov.au/nla.obj-1746260097.
18. Australia, ed., *Report on the Australian Secret Intelligence Service*, Public ed (Canberra: Australian Govt. Pub. Service, 1995).
19. Philip Flood, *Report of the Inquiry into Australian Intelligence Agencies* (Canberra: Dept. of the Prime Minister and Cabinet, 2004).
20. *2017 Independent Intelligence Review* (Canberra: Department of the Prime Minister and Cabinet, 2017).
21. Attorney-General's Department, 'Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community', https://www.ag.gov.au/national-security/publications/report-comprehensive-review-legal-framework-national-intelligence-community.
22. Keiran Hardy, Rebecca Ananian-Welsh, and Nicola McGarrity, 'Secrecy and Power in Australia's National Security State', GetUp Australia, September 2021, https://cdn.getup.org.au/2836-GetUp-Democracy-Dossier.pdf.
23. Malcolm Turnbull, 'Offensive Cyber Capability To Fight Cyber Criminals', 30 July 2017, https://pmtranscripts.pmc.gov.au/release/transcript-41039.
24. Peter Dutton, 'Second Reading Speech - Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020', 3 December 2020, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22chamber%2Fhansardr%2F11b18738-de56-4d82-82f6-2c10fddd6b2b%2F0024%22.
25. Commonwealth of Australia, '*Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*'.
26. James Renwick, *Trust but Verify: A Report Concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and Related Matters* (Barton, ACT: Independent National Security Legislation Monitor, 2020), 18.
27. 'Australia's New Mass Surveillance Mandate', Digital Rights Watch, 2 September 2021, https://digitalrightswatch.org.

au/2021/09/02/australias-new-mass-surveillance-mandate/.
28. John Coyne, 'Encryption: The Perils of "Going Dark"', The Strategist, 27 August 2017, https://www.aspistrategist.org.au/encryption-perils-going-dark/.
29. Department of Home Affairs, 'Surveillance Devices Act 2004 Annual Report 2020-2021', 2021, 35.
30. Department of Home Affairs, 'Electronic Surveillance Reform', 6 December 2021, https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/electronic-surveillance-reform.
31. Australian Civil Society Coalition, 'Submission to PJCIS on the Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018', Digital Rights Watch, 1 July 2019, https://digitalrightswatch.org.au/wp-content/uploads/2019/07/190701-Submission-to-the-Review-of-the-Telecommunications-and-Other-Legislation-Amendment-Assistance-and-Access-Act-2018.pdf.
32. Commonwealth of Australia, 'REDSPICE | Australian Signals Directorate', May 2022, https://www.asd.gov.au/about/redspice.
33. Alex Joske, *Spies and Lies: How China's Greatest Covert Operations Fooled the World* (Hardie Grant, 2022), 200–201.
34. Henry Belot, 'Turnbull to Ban Foreign Donations, Force Agents to Declare International Links', *ABC News*, 5 December 2017, https://www.abc.net.au/news/2017-12-05/turnbull-announces-foreign-interference-laws/9227514.
35. Lisa Murray, 'How ASIO, ASIS and Other Australian Spy Agencies Are Expanding Their Reach', Australian Financial Review, 2 October 2018, https://www.afr.com/life-and-luxury/how-asio-asis-and-other-australian-spy-agencies-are-expanding-their-reach-20180814-h13xsz.
36. John Garnaut, 'How China Interferes in Australia', 5 October 2022, https://www.foreignaffairs.com/articles/china/2018-03-09/how-china-interferes-australia.
37. Burgess, 'Director-General's Annual Threat Assessment | ASIO'.
38. Lowy Institute, 'China as a Military Threat - Lowy Institute Poll', Lowy Institute Poll 2022, June 2022, https://poll.lowyinstitute.org/charts/china-as-a-military-threat.
39. Dina Temple-Raston, 'China's Microsoft Hack May Have Had A Bigger Purpose Than Just Spying', *National Public Radio*, 26 August 2021, sec. Investigations, https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying.