Australian National University

February 2022
ANU College of Law
National Security College

Public Submission - Reform of Australia's Electronic Surveillance Framework

Primary authors:
Dr. Dominique Dalla-Pozza of the ANU College of Law
Dr. William A. Stoltz of the ANU National Security College

About this Submission

This public submission represents the views of the authors alone and not an institutional position on behalf of the ANU College of Law (CoL), the National Security College (NSC), nor the wider Australian National University. The authors alone are responsible for any errors.

This submission is however greatly informed by an ANU CoL-NSC Joint Dialogue held in December 2021 during which a number of scholars from across the ANU reviewed the Department of Home Affair's Discussion Paper and shared valuable insights on the topic of electronic surveillance. The authors would therefore like to thank all the participants of this dialogue for their indispensable contributions to informing this submission, in particular: Professor John Blaxland, Mr. Jake Blight, Mr. Damian Clifford, Mr. Adam Cullen, Mr. Mark Fletcher, Professor Rory Medcalf, Ms. Felicity Millar, Dr. James Mortensen, Mr. Finn Robinsen, and Mr. Sam Williamson.

Introduction

The authors would like to thank the Department of Home Affairs for accepting this submission to the public consultation process concerning potential reforms to Australia's electronic surveillance framework.

The enterprise of consolidating and modernising the legislation that enables Commonwealth agencies to perform electronic surveillance is undoubtedly one of the most complex exercises in national security law reform to be undertaken in the past forty years. The issues to be considered in this initiative also go to the heart of how Australia, as a liberal democracy governed by the rule of law, balances the imperatives of individual liberties with the need to address dynamic external and internal threats to the peace, cohesion, and integrity of Australian society.

The magnitude of the Department's task requires a patient and multi-phased process of consultations, as the Discussion Paper rightly acknowledges.[1] Given this, the authors consider this submission to be only the first step in an on-going dialogue between the ANU academy and the Department throughout the development of these reforms. This submission therefore does not seek to address all aspects of the Discussion Paper. Rather, it seeks to outline a number of key principles and foundational observations that the authors believe should guide the drafting of new electronic surveillance legislation.

Summary of Key Statements

- The Commonwealth should take a holistic appreciation of the harm caused to targets by electronic surveillance to include the impact of retention and dissemination of surveillance material as well as the harm caused by the intrusion of surveillance itself.
- Future legislation should discard current distinctions between types of surveillance material and methods of collection. Whether by means of collecting metadata, live data, retained data or predictive data, all methods of surveillance should be regarded as equally intrusive.
- Rules mandating the destruction of data should be legislated, rather than being defined in procedural, often unpublished internal documents.
- In considering any expansion of agencies with electronic surveillance powers, the Commonwealth should treat such powers as extraordinary and entrust them only to statutory agencies so that enabling legislation can be directly subject to Parliamentary oversight and review.
- A single electronic surveillance agency as a means to manage authorisations and dissemination is unlikely to be effective or feasible.
- The inconsistently defined concept of 'serious crime' in relation to national security threats is blurring traditional distinctions between law enforcement and national security activities in a manner that could undermine public understanding and trust in Commonwealth agencies' use of electronic surveillance powers. The Commonwealth could consider decoupling access to surveillance powers for national security purposes from present definitions of serious crime.

[1] Department of Home Affairs, Reform of Australia's electronic surveillance framework - *Discussion Paper* (2021) p. 7, 74-5 (Hereafter, 'Home Affairs, *Discussion Paper*')

- Despite best efforts, it is unlikely that a truly technology agnostic, completely 'future-proofed' electronic surveillance framework can be realised. Accordingly, future legislation should include a mandated holistic review of the entire framework approximately every ten years or so to enable considered modernisation.
- To support transparency and public understanding of the Commonwealth's use of electronic surveillance powers, future legislation could include a requirement that the government issue an annual statement to Parliament to outline the threats and issues facing agencies that warrant the use of extraordinary powers, including electronic surveillance.
- There is strong merit to a Public Interest Advocate (PIA), but care should be taken to ensure a PIA promotes appreciation of public interest considerations within surveillance agencies themselves because vigilance to abuses of power and regard for the impact of government decision-making on civil liberties are universal obligations for all civil servants and cannot be delegated to a single, external body.

Thank you for taking the time to consider our submission and we look forward to continuing our engagement with the Department's public consultation process.

Sincerely,

Dr. William A. Stoltz
Senior Adviser for Public Policy
National Security College, ANU

Dr. Dominique Dalla-Pozza
Senior Lecturer
ANU College of Law

The Harm of Electronic Surveillance: What Information Can Be Accessed and How Can It Be Accessed

At the core of any surveillance legislation (electronic or otherwise) should be an appreciation that in a liberal democracy surveillance by the state generates a degree of harm. Indeed, it could be argued that the mere possession by the state of surveillance capabilities (regardless of the extent of their actual use) can cause harm by generating a suppressive effect on the free expression of those that fear (correctly or otherwise) that their speech or behaviour is being monitored and by feeding conspiracists' views of an intrusive and pervasive state intent on enabling the misuse of personal information and the curtailment of fundamental rights. These are not trivial concerns especially for a migrant society like Australia where a not insignificant proportion of the community have a collective memory or experience of malicious state surveillance and in an age when social media is readily exploitable by malevolent state and non-state actors.

Central then to considerations of proportionality by legislators enacting electronic surveillance powers and authorities approving their use, should be that the benefits to Australian justice and security of using such powers outweigh the harms caused to the privacy of the individual(s) surveilled in particular, and the potential suppressive effect on free expression in society more generally. In addition, the checks and balances instituted should be robust enough to assure the Australian public that appropriate safety and security precautions are in place.

The potential harms generated by electronic surveillance are made manifold by the ability of digital technology to not only expedite the collection of electronic surveillance material, but to facilitate the generation of powerful investigative insights through the aggregation and technology-assisted analysis of said material, including the prediction of future patterns of behaviour. Accordingly, we believe **future legislation should discard certain current distinctions between types of surveillance material and methods of collection.** Whether surveillance is performed by means of collecting content data, non-content data, historically retained data, intercepted data, or predictive data it breaches the privacy of the target and may curtail the freedom with which they otherwise would have behaved. Assumptions that surveilling a target in real-time is the most intrusive form[2] should be set aside given the potential for artificial intelligence and machine learning to allow analysts to anticipate patterns of behaviour with high degrees of granularity. Given such predictive systems will leverage historic data also means accessing retained information should not automatically be regarded as less intrusive.

Authorisations should therefore consider all forms of electronic surveillance as equally intrusive and as such the Department should consider whether a great deal of the existing warrants could not be consolidated into a single Information Warrant for surveillance against individuals and an Attribute-Based Warrant for surveillance of groups.[3] If this idea is of interest to the Department we would be happy to provide further suggestions, and more detail about how such a system of warrants might work. Furthermore, in considering how electronic surveillance powers should be enacted and used, **the Commonwealth should take a holistic appreciation of the harm caused by electronic**

[2] There is some discussion of this sort of assumption in Sharon Rodrick, *'Accessing Telecommunications Data for National Security and Law Enforcement Purposes,* (2009) 37 Federal Law Review 379, p 384.
[3] Attorney-General's Department, *'Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community'*, n.d., 75, https://www.ag.gov.au/national-security/publications/report-comprehensive-review-legal-framework-national-intelligence-community.

surveillance. In designing and authorising electronic surveillance powers the Commonwealth should consider the harms caused to the privacy of the target through the collection, retention and dissemination of surveillance material as well as the subsequent breach(es) of privacy caused when that material is viewed in-aggregate with other information, including open source and predictive data. [4]

One consequence of this is that, it is imperative that any new legal regime provide guidance about the purposes for which the information obtained via electronic surveillance can be used. We are pleased to see that the Department is giving serious consideration to the 'principles-based' tiered approach and that the Department is contemplating defining the 'ranges' of activities which would be classed a secondary and miscellaneous purposes. [5] However, while the examples of the kinds of purposes that would be classed as 'secondary' and 'miscellaneous' provided in the Discussion Paper are a useful starting point, [6] we caution that these purposes will need to be carefully and as clearly defined as possible. A clear definition of 'purposes' will allow agencies to be confident they are using information properly and will also allow the public some sense of how information which is collected under the new legislation will be used.

It is also pleasing that the Discussion Paper recognises that the new legislative framework will need to include guidance on when information collected by intelligence and law-enforcement agencies will be destroyed. [7] Our preference is that the **rules mandating the destruction of information collected should be included in the legislation itself, rather than for those rules to be located in other procedure documents that are not always publicly accessible.** We believe that Recommendation 126 of the Richardson Review provides a reasonable balance between the need for agencies to retain documents 'for a specified purpose' and the important benefits for people's privacy that a clear mandate to destroy information collected provides. We also think that the test suggested by the Review is a reasonable one; that information be destroyed "as soon as reasonably practicable after the agency is satisfied that the records are not required for a specified purpose (being a purpose for which the information may be used and disclosed), or five years unless the agency positively certifies the records are required for a specified purpose." [8]

However, in the event that the Department decides *not* to include these rules for the destruction of information collected under the new act in the legislation we think the model of a 'mandatory procedure' could be utilised. This model was included in the current version of s 11C of the *Telecommunications (Interception and Access) Act 1979* (Cth) in 2021. [9] In particular, if the rules for destruction of information are to be contained within a procedure, rather than in legislation, it would be essential that this fact be clearly outlined in the primary legislation, that the legislation say that the procedure is 'mandatory' and that a person affected by it 'must comply with it'. [10] It would also be

[4] For discussions of privacy and proportionality which relate to the *Telecommunications (Interception and Access) Act 1979* see Niloufer Selvadurai, Nazzal Kisswani and Yaser Khalaileh, 'The proportionality principle in telecommunications and access law In an environment of heightened security and technological convergence' (2016) 25(3) Information & Communications Technology Law, 229;

[5] Home Affairs, *Discussion Paper*, p 56-7.

[6] Home Affairs, *Discussion Paper*, p 57.

[7] Home Affairs, *Discussion Paper*, p 56-7.

[8] Richardson Review Recommendation 126

[9] As amended by the *Foreign Intelligence Legislation Amendment Act 2021* (Cth)

[10] As is the case in s 11C(8) of the *Telecommunications (Interception and Access) Act 1979*(Cth).

important that the Parliamentary Joint Committee on Intelligence and Security be informed, and may request a briefing, when any mandatory procedure is issued or changed.[11] Finally, if this model is utilised, the legislation should set out that the procedure be subjected to regular review.[12]

[11] As is the case in s 11C(10A) and 11C(10B) of the *Telecommunications (Interception and Access) Act 1979*(Cth).
[12] As Is the case In s 11C(10) *Telecommunications (Interception and Access) Act 1979*(Cth).

The Availability of Electronic Surveillance Powers: Who Can Access Information Obtained by Electronic Surveillance

The Department has asked respondents to consider the feasibility or otherwise of a wider range of Commonwealth agencies being given access to surveillance data and the ability to undertake electronic surveillance independently.

While electronic surveillance data could doubtless assist all manner of Commonwealth agencies, utmost caution should be exercised when considering whether to provision more agencies with such intrusive collection powers, particularly for agencies that are not law enforcement or intelligence agencies. It has been a long-held principle in Australia that **highly intrusive activities by the state should be treated as extraordinary and entrusted to typically statutory agencies for select use to counter the gravest serious offences and threats to Australian security.** Indeed, it was arguably that principle that motivated the 2015 changes to s110 and 110A of the *Telecommunications (Interception and Access) Act* which restricted the law enforcement agencies that could obtain stored communication warrants, and make authorisations under Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* (Cth).[13] Similarly in the PJCIS's 2020 *Review of the Mandatory Data Retention Scheme* the Committee, responding to concerns about the operation of s280(1)(b) of the *Telecommunications Act 1997* (Cth), indicated that it wished

> "to build on and retain confidence in the data retention regime and concludes that the number and type of agencies that can access a person's telecommunications data via section 280 (1) (b) of the Telecommunications Act may undermine the social licence for ASIO and law enforcement agencies to access the information."[14]

That 'social licence' is equally critical to the successful operation of any future Electronic Surveillance legislation. That direct collection of surveillance data would expedite existing operations should not be the sole basis for granting agencies such as the ABF, corrective services, the ATO, and others such powers. These agencies should be made to substantiate, preferably to the Parliament, why the matters for which they wish to use electronic surveillance powers are of sufficient seriousness to Australia to warrant extraordinary powers. In this regard as a general rule **all agencies exercising electronic surveillance powers should be statutory bodies whereby the content and use of their enabling legislation can be subject to regular and public Parliamentary scrutiny.**

Break-down of Law Enforcement-Intelligence Distinction

For much of the period following the establishment of Australia's modern security community post the Second World War, it has been a guiding principle for the drafting of legislation and the creation of policy that there should be a distinction between the Commonwealth powers that can be exercised for the purpose of law enforcement and those that can be exercised for national security. This is in

[13] See the comments of then Attorney-General Senator George Brandis during the parliamentary debates on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 in Commonwealth, *Parliamentary Debates,* Senate, 24 March 2015, 2245. See also Parliamentary Joint Committee on Intelligence and Security, *Review of the mandatory data retention regime* (2020) Parliamentary Joint Committee on Intelligence and Security, *Review of the mandatory data retention regime* (2020) p 117.

[14] Parliamentary Joint Committee on Intelligence and Security, *Review of the mandatory data retention regime* (2020) p 118.

part predicated on an important distinction between collecting evidence of criminal activity that has already transpired for prosecution in the courts, and collection of material for intelligence assessments which tends to be predictive or speculative. This has traditionally manifested in courts and authorising officials treating the collection of evidence and the collection of intelligence as requiring different measures of proportionality and being undertaken via the use of separate powers.

On the one hand the collection of intelligence has been regarded as a less intrusive activity because it cannot be presented in court and therefore cannot aid in the deprivation of liberties that criminal penalties, such as imprisonment, entail. Yet on the other hand, the exercise of intelligence collection is not subjected to the same degree of public scrutiny that evidence, which can be dissected in open court, experiences. The use of 'criminal intelligence' to guide and facilitate the subsequent collection of evidence has further muddled the notion that intelligence cannot lead to as severe outcomes as evidentiary collection.

Admittedly the justice-security or evidence-intelligence distinction has always been somewhat precarious, given that most activities that threaten national security have themselves been criminalised and that law enforcement agencies need to support security agencies in investigating, arresting, and prosecuting national security targets. Exacerbating the challenge is the expectation that predictive intelligence can outwit those intent on criminal behaviour. To help navigate these issues the Commonwealth has traditionally treated national security offences as 'serious crimes' and has delegated national security and law enforcement powers respectively to separate agencies.

Care should be taken with regard to the proximity, similarity and possible overlap between warrants given for the purposes of national security by statutory agencies, and warrants served in the course of law enforcement by police and similar organisations.

There is also a need to ensure a careful balance between effective warrants and safeguarding the distinction between law enforcement and national security as it regards public trust and political legitimacy. As Australia's government is representative, the distinction between the enforcement of the law and the protection of the executive is key to ensuring public trust in political terms, in ensuring that coercive force is not seen to be used by the executive in any but the most pressing of circumstances. Thus without keen sensitivity in the performance of surveillance on Australian citizens by statutory agencies, there is the risk of damaging the perceived legitimacy and accountability of representative government, as well as the perceived of stifling political participation. [15]

In recent times, this distinction between law enforcement and national security powers has been breaking down further particularly in electronic surveillance legislation. This has been driven by two factors. For one, vague and inconsistent designations of 'serious' crimes used to activate special intelligence and evidentiary collection powers, respectively, have created categories of offending that can attract both law enforcement and national security responses in a manner that is obscuring the difference between those serious offences that are of significance to national security and those that

[15] Public Perception of Security and Privacy: Results of the comprehensive analysis of PACT's pan-European Survey (rand.org) and Full article: Political Conflict and Public Perceptions of Government Surveillance on the Internet: An Experiment of Online Search Terms (tandfonline.com)

are not.[16] Secondly, in recent times law enforcement agencies have been provisioned with the power to perform activities for the purpose of generating a national security effect rather than the collection of evidence or criminal intelligence. We are referencing here the Data Disruption Warrants introduced in 2021 which, through amendments to surveillance legislation, provide the AFP and the ACIC with the ability to undertake digital activity against a criminal target solely for the purpose of 'disruption'.[17] Hitherto, such disruption activities otherwise referred to as offensive cyber operations have been the purview of the likes of the Australian Signals Directorate to target actors impacting upon Australia's national security.

We are not contending here that non-security related serious offences do not require special powers but conflating national security threats with serious criminality creates some risks of concern that will likely need to be acknowledged, if not resolved in future legislation. For one, the most expansive definitions of serious crime, including offences attracting 12 months or more imprisonment, captures crimes that likely exceed what many in the community would regard as being an activity impacting upon national security. This could mean that in a most extreme instance, such definitions could facilitate agencies attempting to use national security powers for purposes well beyond the spirit of the law and the intentions of legislators. More likely however is pressure by government and other stakeholders for security agencies to use their finite intelligence collection capabilities across a growing range of crime types, dissipating scarce resources in a manner that risks hampering efforts to address those national security threats that are truly of most concern.

For the purposes of guiding the proportionate use of electronic surveillance powers for national security purposes and revitalising a clearer distinction between national security and law enforcement powers, the Department could consider de-coupling access to electronic surveillance powers for national security purposes from present definitions of serious crime.

The Feasibility of a Single Electronic Surveillance Agency

In developing this submission the authors considered the feasibility of the Commonwealth creating a single electronic surveillance agency (ESA). The idea is that instead of the current system, whereby multiple Commonwealth agencies exercise electronic surveillance powers and manage the corresponding data, a single agency could be instituted to perform electronic surveillance on behalf of approved Commonwealth clients. For example, upon a relevant AFP warrant being approved the ESA would undertake the surveillance, collect the data, sanitise and process the data according to the

---

[16] For the purposes of intelligence collection into national security threats the *Australian Security Intelligence Organisation Act (1979*) (ASIO Act) and the *Intelligence Services Act (2001) (*IS Act*)* each define "serious crime" as offences "against the law of the Commonwealth, a State or a Territory punishable by imprisonment for a period exceeding 12 months". (https://www.legislation.gov.au/Details/C2020C00300) The *Criminal Code Act (1995)* (Criminal Code) also describes a "serious offence" as one penalised by no less than 12 months. (https://www.legislation.gov.au/Details/C2021C00183) However, the *Crimes Act (1914)* describes a 'serious offence' as one that attracts a penalty of 2 years or more. (https://www.legislation.gov.au/Details/C2022C00024) Meanwhile, the *Australian Crime Commission Act (2002)* (ACC Act), which governs Australia's peak criminal intelligence agency, adds further complexity by introducing the concept of "serious and organised crime", being organised offences attracting penalties of 3 years or more. (https://www.legislation.gov.au/Details/C2021C00543)

[17] Commonwealth Parliament, 'Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020', Australia, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6623.

warrant, provide the AFP with the relevant data only, and manage the storage and destruction thereafter.

An ESA could streamline oversight by statutory bodies and the Parliament because only one agency would be responsible for the collection, dissemination, storage, and destruction of original surveillance data. It could also improve public trust by creating a clear 'air-gap' between the collection of electronic surveillance data and those law enforcement and intelligence agencies using said data. Were the function of a Public Interest Advocate for electronic surveillance to be created (as discussed below), such a function could also reside in an ESA.

However, the creation of an ESA could hamper statutory agencies such as the AFP and ASIO undertaking their investigations in a timely and independent manner if the ESA is not appropriately resourced to undertake high-volumes of surveillance requests. In addition, in his royal commission reports, Justice Hope established the principle of the separation of powers between domestic and foreign collection agencies and between collection and assessment agencies for good reason.[18] While arguments for increased efficiency in the short term may be used to undermine this principle, effectiveness and efficacy needs to be weighed carefully as well. Reversing that approach should not be considered lightly. There may be problems with a single entity being responsible for the collection of surveillance data when that data will need to be used for different purposes. For example, as explained above, data that will ultimately be used as evidence as part of an AFP investigation needs to have different qualities than data that is used by ASIO for intelligence purposes. The creation of an ESA would also 'split' the exercise of oversight, which in the case of the Inspector-General of Intelligence and Security typically evaluates the efficacy and probity of an entire investigation, rather than the execution of just one warrant.

On balance, we believe that **the risks associated with the creation of an ESA outweigh any benefits** and so do not think that the new Electronic Surveillance Legislation should create a single ESA.

[18] *'Royal Commission on Intelligence and Security Third Report on Intelligence Co-Ordination Machinery - Abridged Findings and Recommendations,* Dated 1 December 1976', n.d., NAA: A8908, 3B, National Archives of Australia, https://recordsearch.naa.gov.au/SearchNRetrieve/Interface/DetailsReports/ItemDetail.aspx?Barcode=4727805&isAv=N.

Transparency and Oversight

Principles of Oversight

In our view, Australia has a robust intelligence and security oversight regime.[19] There are four principles which are essential to ensuring robust oversight. First, that the agencies and oversight bodies have appropriate leadership; Second, that oversight bodies operate under legislation that gives them sufficient jurisdiction and other powers to ensure they can deliver high quality oversight; Third, that it is vital that internal oversight mechanisms (such as authorisation processes) and external oversight mechanisms (such as ombudsmen, inspectors general and independent monitors) are staffed with the appropriately skilled staff and sufficiently resourced; Last, an understanding of the critical nature of maintaining public trust in both the intelligence and law enforcement bodies and the oversight bodies themselves.[20]

The authors assert while public trust In Australia's oversight bodies is high, it is also fragile.[21] It is absolutely appropriate that the new Electronic Surveillance Legislation contain provisions which ensure that the collection, use, retention and destruction of data for surveillance purposes be monitored by oversight bodies and mechanisms.[22] Indeed, the creation of a new electronic surveillance legislative framework nevertheless presents opportunities for improvement.

Public Reporting and Engagement

One aspect in which Australia is lacking in comparison to other Five Eyes countries is in public transparency.[23]. In part this reflects the different constitutional models employed in a federal bicameral Westminster style parliamentary democracy. But with much of the US experience reflected in Australia news media, a growing expectation of transparency and public accountability has emerged. Not being part of the legislative branch, and falling under distinct bureaucratic authority and sometimes buried under overarching government management arrangements, Australia's agencies can still exercise a high degree of risk aversion to engaging in public discussions regarding their capabilities, operations, and internal deliberations; presumably out of concern for disclosing sensitive capabilities, compromising active investigations, or risking being embarrassed for saying the 'wrong' thing in an unforgiving 24 hr news cycle. However, in the context of agencies seeking to gain, use, and retain electronic surveillance powers we believe it should still be possible for agencies to discuss their operations and capabilities in a sufficiently sanitised, unclassified manner.

In the course of this consultation process and in subsequent annual reporting to Parliament on the use of their electronic surveillance powers, it is vital to the sustainment of public trust that agencies explain publicly their need for these powers and how they intend to use them. For this reason, the

[19] See the discussion provided in Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Independent Intelligence Review*, pp 111- 2 and Dennis Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community Volume 3: Information, Technology, Powers and Oversight* (2019) pp 256-7.,
[20] Notes from NSC-CoL Dialogue.
[21] Notes from NSC-CoL Dialogue.
[22] Home Affairs, *Discussion Paper*, p 63.
[23] See for example, the comparisons made by the former Independent National Security Legislation Monitor, Dr James Renwick between data released by the United Kingdom Home Office which relates to 'the number of counter-terrorism arrests, convictions and acquittals and details of the sentences', and the discussion that follows see: Independent National Security Legislation Monitor, *Annual Report 2018-2019* (2019), pp.xi-xii.

authors hope to see the Department's public engagement efforts complimented by initiatives from agencies themselves. The incumbent Director-General of Security's decision to release an Annual Threat Assessment, supported by a press briefing[24], is an example of a positive change but one that ideally should be regarded as the norm, not the exception.

To support transparency and public understanding of the Commonwealth's use of electronic surveillance powers, **future legislation could include a requirement that the Prime Minister or Minister for Home Affairs issue an annual statement to Parliament to outline the threats and issues facing agencies** that warrant the use of extraordinary powers, including electronic surveillance. The Director General of Security has modelled this approach with the annual ASIO threat assessments. This approach conceivably could be elevated to prime ministerial level statement to Parliament

Silence from agencies cedes the public story about their activities to other voices that are not always adequately informed. This presents the unacceptable risk of mis- and disinformation regarding agencies forming the basis for the public's understanding of what is being done in their name. It needlessly overlooks the opportunity to include the Australian public as an important part of the narrative for a safe and secure nation.

Review of Legislation

The existing electronic surveillance framework has been built up sporadically over decades to span multiple pieces of legislation enacted in different eras to meet different operational challenges. The result is a labyrinthine web of laws, a 'house of cards' that is so difficult to navigate that only a comparatively small number of seasoned operational and legal professionals within the government can do so with a high degree of confidence. [25]

The paucity of a comprehensive approach to understanding and amending the existing framework has exacerbated the tendency of policymakers to seek 'quick fix' amendments for pressing operational challenges, in turn producing more confusion and at times contradictions within the framework.

In this context, the intention of the Department to holistically re-evaluate and replace the existing framework is commendable. However, it should be carried out with an appreciation that how ever much the Department may try, the accomplishment of a truly technology-agnostic, completely 'future-proofed' framework is unlikely to be realised due to the dynamism of Australia's operating environment and the sheer speed of technological change that is unlikely to abate in coming decades. Therefore, an important objective for the Department should be to avoid the creation of a new framework that will either unduly inhibit future options or simply become another 'house of cards' that in a generation hence, the Department's successors will have to untangle yet again.

[24] See Mike Burgess, *Director-General's Annual Threat Assessment* 9 February 2022 (Canberra) < https://www.asio.gov.au/publications/speeches-and-statements/director-generals-annual-threat-assessment-2022.html> and press coverage of the speech such as Daniel Hurst, ' Violent extremists': Asio boss warns of 'angry and isolated' Australians radicalised during pandemic' , 9 February 2022, *The Guardian (Australian Edition) Online* < https://www.theguardian.com/australia-news/2022/feb/09/violent-extremists-asio-boss-warns-of-angry-and-isolated-australians-radicalised-during-pandemic?CMP=Share_AndroidApp_Other>

[25] See the discussion of the complexity of the current interception framework In Dennis Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community Volume 2: Authorisations, Immunities and Electronic Surveillance* (2019) pp 260-2.

One way this may be done could be to build a review period into the new electronic surveillance legislation to **mandate that every 10 or 15 years the act should be comprehensively reviewed by the Parliament.** A review period of this length would be frequent enough to evaluate the framework in-light of technological or operational developments unprecedented at the time of drafting, but not so frequent as to become a hinderance. Furthermore, a regularised comprehensive review of the framework would allow policymakers to better triage the near constant stream of amendments that has characterised the previous legislative era.[26] Knowing the entire framework will be subject to a review every decade or so will give governments the option to hold-over less urgent amendments that can be risk-managed until they can be considered in a more comprehensive context. In-turn Parliament could prioritise the resolution of operationally urgent legislative issues that cannot be risk-managed.

It could be argued that such a regularised review of the framework could subject the Commonwealth's electronic surveillance regime to the re-prosecution by interest groups and agencies of matters previously 'settled'. However, the reality is that re-prosecution of old debates is inevitable as none of the questions relating to the state's use of intrusive powers are ever 'settled'. Just as the technological and operating environments will constantly shift, so too will Australians' social mores and attitudes to the functions of government be subject to change. What Is more, that change may be antithetical to the government's interests if the national security and law enforcement agencies do not adequately engage in the public debate. Given this, the regularised comprehensive review of this important framework would also serve to aid public understanding and debate and in so doing contribute to oversight of the framework itself.

[26] See the discussion of the Australian 'tradition of independent periodic reviews, inquiries and commissions that drive regular change and innovation in the scope and structure of accountability' in Christian Leuprecht and Hayley McNorton *Intelligence As Democratic Statecraft* (2021) Oxford University Press, 156.

A Public Interest Advocate and Special Protections

The Department has asked about the need for a Public Interest Advocate (PIA) as well as the potential utility of providing special protections for specific classes of persons.

Nominating classes of persons for special protections with regards to electronic surveillance, whether they be journalists, clergy, lawyers, politicians, or doctors, is inconsistent with the principle that all people are equal before the law. If an agency has due cause to suspect someone of an offence warranting the use of electronic surveillance, the vocation of that individual should be immaterial.

The suggestion of special protections appears to be based on the premise that there are people in society performing functions deemed to be of a particularly essential value to Australian society and that therefore their privacy and freedom of expression warrants additional protection beyond that of an ordinary citizen. In developing this submission, the authors discussed the potentially more abstract alternative approach of providing special protections for these essential functions themselves, rather than the individuals performing them. For example, instead of requiring agencies to provide additional justifications to perform electronic surveillance on a target that happens to be a journalist (even when the offence being investigated may have nothing to do with their employment), an agency could be made to factor into their assessments of proportionality whether or not the act of surveillance will have an impact on the proper functioning of a journalistic institution. This approach would be closer to maintaining individuals' equality before the law and would follow the precedent of parliamentary privilege whereby investigations must not interfere with the conduct of Parliamentary business, but this does not universally indemnify parliamentarians from being investigated like an ordinary citizen for matters unrelated to their parliamentary business.[27] Such a model would still present challenges, such as determining which functions justify special protections and how to incorporate such protections into a warrant approval process without hampering operational imperatives.

Despite these challenges, we believe a PIA empowered to make submissions as part of a warrants process would be an important accountability mechanism to include in the new Electronic Surveillance legislative framework. However, we wish to sound a note of caution. The adoption of a PIA as part of the new framework *should not* relieve the government officials who are charged with making decisions about whether to apply for permission to obtain such data, or to approve such requests from *their own* obligations to exercise due consideration for a wider range of public interest considerations beyond the operational objectives of their particular investigation.

Accordingly, we believe a PIA should be seen as an *additional* safeguard allowing decision makers access to alternative arguments about why a request for surveillance data should (or should not) be approved. The creation of a PIA should not generate the perverse outcome of inculcating a permission structure for law enforcement and intelligence officials to forgo certain ethical considerations about the proportionality of their behaviour on the assumption that such considerations have been delegated to a PIA. In this regard, the Department may wish to consider a PIA model whereby officials with PIA responsibilities are both external to and embedded within relevant agencies, akin to how

[27] Parliament of Australia, *'Guides to Senate Procedure - No. 20 - Parliamentary Privilege',* n.d., https://www.aph.gov.au/About_Parliament/Senate/Powers_practice_n_procedures/Brief_Guides_to_Senate_Procedure/No_20.

despite the existence of external oversight and integrity bodies agencies still maintain their own in-house compliance and assurance specialists.

Vigilance to abuses of power and regard for the impact of government decision-making on civil liberties are universal obligations for all civil servants whether they be an investigator or an oversight officer. If there are concerns about the integrity with which certain civil servants or agencies exercise these obligations they are unlikely to be resolved completely by statute as they are more likely to be issues of APS training or culture. In the realm of national security and policing, reputation matters enormously to public confidence and trust, regardless of whether this reputation is based on perception or reality. With increased prospects of political interference, manipulation of social media and distortions abounding, the need for greater transparency and active engagement is more important than ever. Accountability must be seen to be a major feature of the national security and law enforcement domains.

About the Authors

Dr. Dominque Dalla-Pozza

Dr. Dalla-Pozza is a Senior Lecturer in the Law School at the ANU College of Law, ANU.

She has published on various aspects of the development of the Australian counter-terrorism law framework as it has been developed since 2001. She is particularly interested in the workings of the Australian bodies that provide national security oversight.

Dr Dalla-Pozza holds a PhD in Law from the University of New South Wales as well as combined Bachelor of Arts/Bachelor of Laws degrees from the University of Sydney.

Dr. William A. Stoltz

Dr. Stoltz is the Senior Adviser for Public Policy at the National Security College, ANU. He is responsible for mobilising the College's research and resident expertise to influence and inform current public policy debates.

Dr. Stoltz's own research explores options for Australia to shape and influence international security, as well as Australia's policy responses to a breadth of domestic national security challenges.

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.