SALUS JOURNAL

Volume 12, Issue 1, 2024
ISSN: 2202-5677

Privacy and Hacking Powers: Is there an Implied Right to Privacy in the Use of Computer Surveillance Powers in Australia?

Dr Brendan Walker-Munro, Ms Ruby Ioannou, Dr David Mount

Research Article

ABSTRACT

On 3 September 2021, Australia's Commonwealth Parliament passed the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Cth). In doing so, it added to an already expansive regime of warrants and authorisations, enabling law enforcement and intelligence officers to break into, search, seize and even destroy computers, devices, or networks. These powers are largely untested in terms of judicial appeal and administrative review and are some of the most privacy-intrusive powers given by any legislation anywhere in the world. In examining the scope and interference enabled by these powers, we conclude that officers seeking warrants to hack into or damage computers, devices or networks in Australia have an implicit duty to consider the effect of their actions on the suspect's privacy.

Keywords: *hacking, privacy, national security, law enforcement, Commonwealth law.*

INTRODUCTION

Our article considers whether the use of intrusive computer surveillance powers in Australia is currently limited by a test that the use of the power is 'reasonable, necessary and proportionate' when measured against the interference with privacy of the suspect. In particular, the use of law enforcement powers to hack into offenders' computers, devices or networks (CDNs) located domestically is one of the most intrusive powers available to the Australian law enforcement and intelligence community and should therefore be attended by the strongest safeguards and protections. In doing so, we consider whether the laws (properly constructed) ought to place the onus of proof on law enforcement or intelligence agencies before they seek to execute such powers.

Volume 12, Issue 1, 2024
ISSN: 2202-5677

The reason for our focus on an implicit duty to consider interference with privacy can draw its genesis from the earliest limitations on the execution of State power in the English case of *Entick v Carrington* (1765). There, a warrant issued by Lord Halifax, a member of the Privy Council and Secretary of State, was struck down by Lord Camden, Chief Justice of the Common Pleas. In doing so, not only was a cornerstone principle established in constitutional law that limited the scope of executive power, but his Lordship also recognised the boundaries of appropriate curtailment on officers of the Executive in infringing the rights of the common populace. His Lordship said:

> A power to issue such a warrant as this, is contrary to the genius of the law of England…it is the publishing of a libel that is a crime, and not the having it locked up in a private drawer in a man's study; but if having it in one's custody was the crime, no power can lawfully break into a man's house to search for evidence against him; this would be worse than the Spanish Inquisition; for ransacking a man's secret drawers and boxes to come at evidence against him, is like racking his body to come at his secret thoughts.

The export of this concept to the protean United States at the time of colonisation led lawyers Samuel Warren and Louis Brandeis to infamously remark that technological advancements in the form of 'instantaneous photographs and newspaper enterprise[s]' were 'invading the sacred precincts of private and domestic life' (Warren & Brandeis, 1890).

The groundswell of domestic laws passed by States to recognise the right to privacy in the nineteenth and early twentieth centuries (Hauch, 1994) no doubt inspired the international community to codify the practice in the Universal Declaration of Human Rights (UDHR, 1948). Article 12 states that '[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation' and provides the full protection of the law to all against such interference or attacks. Further international treaties and enactments over the past seventy years have all used a common language invoking full protection of the law against such 'arbitrary interference or attack' of privacy.[1]

Following the establishment of the European Convention on Human Rights (ECHR) and the creation of the European Court of Human Rights (ECtHR) to enforce it, the ECtHR has taken great steps to provide commentary on the scope and contours of privacy as a human right protected by international law (Strossen, 1990). Of relevance here, the early decisions of the ECtHR on surveillance by States made it clear that Article 8 of the ECHR would be interpreted broadly, such that privacy under international human rights law ("IHRL") became synonymous with the concept of 'the right to live, as far as one wishes, protected from publicity…[i]t comprises also, to a certain degree, the right to establish and develop relationships with other human beings, especially in the emotional field for the development and fulfillment of one's own personality' (*X v Iceland*, 1976). Mere collection of sensitive information will invoke the protection

[1] The full list of UN Conventions containing such protections is included in the References.

Volume 12, Issue 1, 2024
ISSN: 2202-5677

of IHRL, as would using sensitive information for a purpose not consistent with the purpose of that collection (*Leander v Sweden*, 1987).

More recent decisions by the Strasbourg court have expanded even that broad reach of privacy to incorporate the capacity for private citizens to control the use and registration of their personal information (De Hert & Gutwirth, 2009). These cases have included those involving allegations of abuses of power by States using intrusive surveillance systems against their own citizens (*Klass & Ors v Germany*, 1979; *Leander v Sweden*, 1987; *Cyprus v Turkey*, 2001). That baseline assumption of a positive right has flavoured the EU experience of privacy regulation, where the focus on human rights incorporated broader rights into the digital ecosystem, such as the right of erasure and the right of refusal of processing (Mayer-Schonberger & Padova, 2015).
Australia has no Human Rights or Civil Liberties Act in its federal jurisprudence with which to constrain privacy abuses, and judges 'do not acknowledge an overt influence of international human rights obligations on the Australian common law' (Witzleb, 2020, p. 775). Instead, Australia's legal approach to the protection of its citizens' privacy favours legitimate commercial or public interests over the rights of the individual, and reform in the opposing direction has been slow (Lindsay, 2005, p. 159):

> For the pioneers, the United States and Sweden, the convergence resulted from independent and indigenous analyses that travelled along the same learning curve and arrived at the same conclusion. For West Germany, and other countries such as Canada, France, Norway, Denmark and Austria that legislated in the late 1970s, the convergence followed from the mutual process of lesson drawing within an international policy community. For Britain, and other laggards such as the Netherlands, Japan, and Australia, the convergence has resulted from the pressure to conform to international standards for mainly commercial reasons.

Australia on the other hand approaches privacy as a normative construct for business, accepts that they will breach privacy in the collection of personal information, and seeks to enact safeguards around that collection and use (Lindsay, 2005, p. 153).

That said, High Court jurisprudence has established a line of authority that the entry into and ratification of an international treaty obliges both the courts and executive to favour constructions that accord with Australia's international obligations (*Minister for Immigration and Ethnic Affairs v Ah Hin Teoh*, 1995). Therefore, Australia is a unique case study for undertaking this examination, as it both lacks constitutional protections or remedies for privacy (Mann et al., 2018) but has also participated in large-scale global surveillance practices via the Five Eyes intelligence sharing alliance (James, 2018).

This paper thus argues that, in accordance with both international human rights law and Australian domestic law, security and intelligence agencies have at least an implicit obligation (in the absence of an explicit obligation) to assess the reasonableness, proportionality and necessity of their intrusion into a suspect's CDNs when exercising their "hacking powers".

Following this initial section, Part 2 will examine the current field of law applying to surveillance and intrusion warrants as they apply to CDNs and describe the nature of the existing

Volume 12, Issue 1, 2024
ISSN: 2202-5677

obligations on law enforcement and intelligence operatives in seeking such warrants. From a practical perspective, Part 3 offers an examination of the tests for necessity, reasonableness, and proportionality to warrants sought under that legislation. In doing so, we aim to advance the thesis that law enforcement and intelligence operatives carry at least an implicit need to satisfy those criteria before the obtaining of such warrants. Part 4 then concludes with some observations for potential law reform (to make such obligations clearer) and areas of future research on this topic.

AUSTRALIAN SURVEILLANCE LAWS AND CDNs

We now turn to the legislative frameworks that regulate the use of intrusive computer activity in Australia. There is no single piece of legislation that regulates the manner of intelligence and law enforcement agencies gaining access to CDNs as part of their duties. Although many of the provisions of the Surveillance *Devices Act 2004* (Cth) (SDA) will be relevant, there are equally powers granted to agencies which fall under the *Intelligence Services Act 2001* (Cth) (ISA), powers given under the *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act), and those afforded to the Australian Federal Police under the *Crimes Act 1914* (Cth) (Crimes Act). Australia's Defence Force may also be given certain powers to access CDNs under the provisions of the Part IIIAAA of the *Defence Act 1903* (Cth) (the Defence Act) (noting that these inevitably require certain declarations by the Governor-General as to a state of domestic violence or threat).[2]

In the interests of scoping, we intend to deal only with acts of agencies which involve access to CDNs in a manner that either involves a covert methodology or tactic and is unknown to the owner of the computer, device or network, or alternatively, in a manner which is not consented to by the owner of the computer, device or network. Given that scope, it is largely irrelevant – at this stage – whether such access is sought for gathering intelligence, the collection of evidence of criminal offences, or the pursuit of a military objective. In all three cases, it is the nature of the access against both the knowledge and consent of the owner which is relevant.

Offshore CDN surveillance

Agencies established under the ISA include Australia's Secret Intelligence Service (ASIS), the Australian Signals Directorate (ASD), as well as the Australian Geospatial-Intelligence Organisation (AGO) and Defence Intelligence Organisation (DIO). These various agencies collectively possess a mandate to collect information and produce intelligence on subjects located outside of Australia (ISA, ss 6(1)(a), 6B(1)(a) and 7(1)(a)). Even though these agencies may "cooperate" with Commonwealth, State and Territory entities – including police and military

[2] Which is separate from the Governor-General's prerogative – as the King's agent – to order the defence of Australia in the manner he or she sees fit (Moore, 2017, p. 169).

Volume 12, Issue 1, 2024
ISSN: 2202-5677

forces – they are nonetheless precluded from cooperation where it is not relevant to the performance of that agency's functions under the ISA (ISA, s 13(1)).

The framework of authorisation for agencies constituted under the ISA is an exercise in Ministerial power, not judicial. The ISA stipulates that the responsible Minister for ASIS, AGO, and ASD must issue a written direction circumscribing the production of intelligence or operations with a direct effect on Australian persons unless an authorisation must be sought. Several observations can be made about the exercise of ISA powers to conduct computer surveillance.

First, the effect of the Ministerial direction and authorisation scheme is only to protect the interests of an 'Australian person', being either a citizen or permanent resident (ISA, s 3). All other persons outside Australia are – irrespective of their connection with Australia – fair game for the purposes of those ISA agencies. Second, an authorisation is only required in circumstances where the planned activities of the ISA agency denote the production of intelligence, the provision of assistance to military operations by the Australian Defence Force (ADF), or disruption of cybercrime (ISA, s 8(1)). Any exercise of an ancillary or tangential function by an ISA agency, or where the 'outside Australia' caveat does not exist, therefore do not require Ministerial approval. Third, there are several instances in which Ministerial approval under a direction does not need to be sought, such as in the absence of the relevant Minister or the Attorney-General, or in the case of imminent risk to the safety of an Australian person (ISA, ss 9B, 9C and 9D).

Most importantly, a Ministerial direction cannot be issued where the ISA agency seeks to undertake 'prescribed activities', which includes those which could be authorised by warrants under the ASIO Act or the *Telecommunications (Interception and Access) Act 1979* (Cth). Assuming that an activity sought to be undertaken by an ISA included accessing a computer, device or network outside the terms provided by those Acts, the Minister would still need to be satisfied that 'there are satisfactory arrangements in place to ensure that the nature and consequences of acts done in reliance on the authorisation will be reasonable, having regard to the purposes for which they are carried out' (ISA, s 9(1)(c)).

Onshore CDN surveillance

Operating within Australia, the surveillance of CDNs is likely to be undertaken by ASIO and the Australian Federal Police (AFP). There may also be occasions when the Australian Crime Commission (in conjunction with the Australian Criminal Intelligence Commission (ACIC) or newly minted National Anti-Corruption Commission (NACC)) may also undertake relevant surveillance, as they are also considered 'law enforcement bodies' for the purposes of the SDA.

ASIO's powers flow from the granting of warrants under the ASIO Act. Of relevance to this article is power of the Director-General of ASIO to seek a warrant from the Attorney-General if:

> ...he or she is satisfied that there are reasonable grounds for believing that access by the Organisation to data held in a computer (the target computer) will substantially assist the

Volume 12, Issue 1, 2024
ISSN: 2202-5677

> collection of intelligence in accordance with this Act in respect of a matter (the security matter) that is important in relation to security (ASIO Act, s 25A(2)).

Again, this is the exercise of Ministerial power, not judicial. The level of satisfaction to be reached by the Attorney-General is a test of reasonableness, as to the "reasonable grounds" requirement for the data stored on the target computer, the security matter being investigated by ASIO, and the requisite connection between the two. There is no actual explicit test which invokes either necessity or proportionality.

Nor is necessity or proportionality explicitly required for other warrants under the ASIO Act which might authorise the surveillance of a targeted CDN. For example, the Attorney-General may issue an identified person warrant if he or she is reasonably satisfied that a named person is 'involved in activities prejudicial to security' (ASIO Act, 27(2)). Under this form of warrant, ASIO has conditional access to that person's CDNs, assuming that the access or collection is consistent with the purpose for which the warrant was granted.

Foreign intelligence warrants – those which target 'foreign intelligence' rather than matters of 'security' – similarly lack a stated requirement for necessity or proportionality (ASIO Act, s 27A). However, there is an implicit test of necessity imposed by the need for the Attorney-General to receive advice from either the Defence Minister or Foreign Affairs Minister before granting the warrant. In both cases, necessity arises because the relevant Minister must attest that the subject matter of the warrant is 'in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being' (ASIO Act, s 27A(1)(b)). An application for a warrant which does not address the necessity of the collection within those terms must fail.

The remaining scope of surveillance of CDNs comes then from the law enforcement and intelligence activities of the AFP, ACIC, and NACC (as well as State and Territory police and integrity bodies) under the SDA. Under that framework, activities may be authorised by a surveillance device warrant, computer access warrant, a data disruption warrant, or a network activity warrant.

In all four warrant applications, there is a degree of consistency across the statutory tests before issue. An application must be made to an eligible judge or nominated member of the Administrative Appeals Tribunal (AAT), who may grant the warrant sought if there are 'reasonable grounds for the suspicion founding the application', and in the case of unsworn or remote applications, there was some circumstance which rendered a sworn, in-person application impracticable. Interestingly, at the stage at which the application is made, both a data disruption warrant and a network activity warrant impose additional tests that the eligible judge or AAT member is reasonably satisfied that the target of a data disruption warrant is 'reasonably necessary and proportionate' (with regard to the offences being addressed by the warrant), and that the analysis of network activity is 'justified and proportionate' (with regard to the offences being addressed by the warrant; SDA, ss 16(2), 27C(2), 27KC(2) and 27KM(2)).

Volume 12, Issue 1, 2024
ISSN: 2202-5677

The SDA also establishes a series of things to which the relevant eligible judge or AAT member must have regard, which (relevant to this paper) include an examination of the extent of interferences with the privacy of any persons, as well as whether alternative means or methods might obtain the evidence or information sought under the warrant.

Military CDN surveillance

The final organ of State which might seek to conduct computer surveillance by way of hacking is the ADF, which has – publicly at least – possessed a computer-based information warfare capability since 2017 (Austin, 2017). The scope of military activities undertaken offshore is notoriously difficult to assess and is in many cases irrelevant.

What does become relevant is the scope of power afforded the ADF under a state of domestic emergency contemplated by the Defence Act (Letts & McLaughlin, 2019). This Act permits the Governor-General – either in response to a request from a State or Territory or to protect Commonwealth interests – to "call-out" the ADF (Defence Act, ss 33 and 35). Even though the ADF would notionally be acting in concert with other organisations from the Commonwealth, States and Territories, the ADF remains under the command of the Governor-General. The Governor-General may also choose to deploy the ADF under the doctrine of necessity, in which Australia merely acts to protect its own interests by 'responding to emergencies or keeping the peace' (*Burmah Oil Co Ltd v Lord Advocate*, 1965; *R v Secretary of State for the Home Department; Ex parte Northumbria Police Authority*, 1989). However, such a deployment will inherently limit any purported reliance on the statutory provisions of the Defence Act in the pursuit of their duties (Lippis, 2022, p. 648).

The nature of a military deployment inside the territorial confines of Australia matters, because it has the effect of constraining the activities open to the ADF's hacking capabilities. If the Governor-General issues a call-out under the Defence Act, the Minister for Defence may issue a written authorisation which permits the use of particular powers that include the operation of electronic equipment 'in a particular manner' (Defence Act, s 46(7)(j)). Equally, the use of such capabilities may devolve to a command decision, either in defence of a specified area or declared critical infrastructure. The only tests for reasonableness and proportionality are if the use of those capabilities amounts to a 'use of force' against a person (Defence Act, s51N(1)).

On the other hand, if the ADF were deployed under a call-out order in response to a law enforcement problem, the exercise of all powers under Part IIIAAA of the Defence Act becomes subject to a test of reasonableness and necessity to achieve the purpose of that order.3 A member of the ADF is also only permitted to exercise powers afforded under the call-out order

[3] Defence Act, ss 33(3), 34(3), 35(3) and 36(3). The obligation is imposed by s 39(2), and subject to ss 39(3) and 40.

Volume 12, Issue 1, 2024
ISSN: 2202-5677

where a request in writing has been made by the State or Territory police. Even where call-outs have been effected using constitutional power or the prerogative of the Crown, the use of military forces to achieve law enforcement outcomes is highly questionable, and in the absence of clear High Court authority, should not be relied upon except as a last resort (Gray, 2021).

Nor is the ADF strictly able to rely upon the ASD (which counts Australian military personnel among its complement) to assist. Although cooperation between the ADF and the ASD is contemplated under the Defence Act and the ISA, it is reasonably arguable that this was not intended to apply to the use of hacking capabilities *inside* Australia. The issue of an order of the Governor-General (or the Chief of the Defence Force for that matter) to the military personnel of ASD to perform some activity outside the scope of the ISA is not only unlikely, but sure to prompt a constitutional crisis. Equally, the fact that the ADF is not a law enforcement agency and does not count law enforcement among its core functions should eschew attempts to "shoehorn" a request between the ASD and the ADF into the cooperation provisions in section 13 of the ISA.

APPLYING NECESSITY, REASONABLENESS AND PROPORTIONALITY TO THE HACKING POWERS

Having considered each of the Commonwealth laws which seek to regulate law enforcement and intelligence access to CDNs, we now consider whether the hacking powers outlined in Part 2 are subject to an implicit requirement to consider the necessity, reasonableness, and proportionality of those powers in the face of the interference with the suspect's privacy. In doing so, we consider that the application of necessity, reasonableness, and proportionality is a key ingredient to the granting of such extraordinary powers to our law enforcement and intelligence agencies. Indeed, it was said that 'the extent of the intrusion into privacy…should be correlative to the security issue at stake' (Hope, 1977, p. 148).

For that purpose, we identify that data disruption warrants sought under the SDA already carry an explicit test for necessity, reasonableness, and proportionality. Data disruption and network activity warrants are statutorily limited to law enforcement officers of the AFP or Australian Crime Commission. In both the case of a "data-based disruption warrant" (which seeks to disrupt target data in a CDN) or an "offence-based disruption warrant" (which seeks to frustrate a particular offence or offences), the application requires endorsement from a senior officer with 'relevant skills, knowledge, and experience to endorse the making of applications for the issue of data disruption warrants' (SDA, ss 27KBA(4)(b) and (5)(b), 27KBB(4)(b) and (5)(b)). For both data disruption and network activity warrants, the judge or AAT member must also then turn their mind to whether the activities authorised by the warrant are 'reasonably necessary and proportionate, having regard to the offences' listed.

Necessity

Volume 12, Issue 1, 2024
ISSN: 2202-5677

Necessity contemplates an element of foresight as to the intrusion likely to be occasioned, meaning that a citizen or resident in Australia should be able to know in advance under what conditions the State may abrogate or interfere with their rights (Anderson, 2015, p. 13.31). Necessity also requires that practices which intrude upon the norm of privacy only be considered defensible where a State deems them necessary to achieve a legitimate aim (*Toonen v Australia*, 1994). The Strasbourg courts have interpreted this principle as read down to only authorise intrusions which are justified by 'strict necessity' (*Szabo v Vissy Hungary*, 2016).

Such an approach concords with protecting the right to privacy under international law. For example, the International Covenant of Civil and Political Rights prohibits any person being 'subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation' (ICCPR, art 17). The critical aspect of that provision is the invocation of the terms "arbitrary" and "unlawful", placing the obvious onus on those doing the interfering to prove that their actions are both selective enough by reference to the suspect but also supported by law. That has been interpreted under international law to include permissions to live without publicity and freedoms within the community (*Airey v Ireland*, 1979).

Arbitrary or unlawful interference connotes 'elements of injustice, unpredictability, unreasonableness, capriciousness and unproportionality', such that any interferences or restrictions on the right to privacy by law must be adequately articulated within a legal framework that is 'publicly accessible, clear, precise, comprehensive, and non-discriminatory' (Nowak, 1993, p. 178). Frameworks which contain 'secret rules and secret interpretations of law', or those which unfairly invoke the principle of 'national security' are offensive to this principle, as are those that do not involve free and fully informed consent for collection (Willoughby, 2017, p. 44).

The nature of hacking powers under the various pieces of Commonwealth legislation requires an implicit consideration of necessity as to the intrusion of the suspect's privacy. As a reference point for that necessity, many Australian intelligence agencies publish publicly available Privacy Rules as a mandated requirement. For example, the privacy rules applying to the Defence Intelligence Organisation (DIO) embed a need for necessity before the collection, retention, and communication of intelligence information relating to Australian persons (Defence Intelligence Organisation, 2023). The DIO privacy rules also explain the assumptions which apply to whether someone is, or is not, considered an Australian person to whom a Ministerial direction or authorisation might apply. Rules 2 and 3 also require necessity in retaining, handling, and communicating intelligence information with 'the proper performance of DIO's functions or…authorised or required by or under another Act'.

Allowing for small variations, the Privacy Rules for other intelligence agencies are all identical (Australian Geospatial-Intelligence Organisation, 2012; Australian Signals Directorate, 2021; Australian Secret Intelligence Service, 2021; Office of National Intelligence, 2022). The Information Handling Protocol enacted by the ACIC (Australian Criminal Intelligence

Volume 12, Issue 1, 2024
ISSN: 2202-5677

Commission, 2020) and Minister's Guidelines to ASIO (Dutton, 2020) equally impart obligations of necessity around the pursuit of those agencies' functions.

Even in the absence of formalised privacy rules, obtaining a warrant related to hacking powers – whether under the ISA, the SDA or other legislation discussed in Part 2 – requires respect of that principle of necessity. The language of limiting infringement of privacy to the extent necessary is inherent in both the application for and execution of a computer access warrant, as well as the satisfaction of the Minister issuing an authorisation under the ISA. Although necessity is not a feature of a computer access or identified person warrants for ASIO, they nonetheless require the satisfaction of the Attorney-General that the activities contemplated would 'substantially assist' the collection of intelligence relevant to security (ASIO Act).

For both warrants, it would further be required to demonstrate that the necessity of the intrusion counterbalances the privacy of the suspect to the degree that doing so would "substantially" assist (rather than merely being useful or incidentally helpful), as privacy does not automatically yield to security (Bronitt & Stellios, 2005). Finally, the broad powers of the military under a call-out order are curtailed to the extent that they engage only necessary infringements to privacy, as the Chief of the Defence Force is subject to an overarching obligation to deploy the ADF 'in such manner as is reasonable and necessary' (Defence Act, s 39).

Reasonableness

Reasonableness, contrary in some respects to necessity and proportionality, is a subjective and not objective assessment. To test for reasonableness is to consider whether, at the time of the question and on the information associated within it, the decision made, or course taken was adapted to be purposeful to its intended outcome. In the public law decisions relating to searches, reasonableness is often characterised by the awareness and state of mind of the officer applying for the authorising warrant, who recounts – as best and as accurately as he or she knows it to be – the circumstances grounding the application (*R v Peirson*, 2014; *R v N*, 2015).

In some respects, the prospect of reasonableness can be analogised to the concept of probable cause in US jurisprudence. There, the Fourth Amendment to the US *Constitution* prohibits "unreasonable" searches and seizures, requiring probable cause (or acts of serious emergency) before the exercise of intrusive investigations by officers of the State (Corn, 2013). Nor is the notion of reasonableness a mere academic concern. Empirical studies have demonstrated that the reasonableness of a search matters a great deal contextually to the perceived intrusiveness (Blumenthal et al., 2008; Slobogin & Schumacher, 1993).

In *Minister for Immigration and Border Protection v SZVFW* (2018, p. 720) the High Court held that a decision to exercise a statutory power is unreasonable where it 'lacks an evident and intelligible justification'. Thus, to determine whether the exercise of a hacking power was reasonable would require satisfaction that there was a cogent and justifiable basis for seeking

Volume 12, Issue 1, 2024
ISSN: 2202-5677

the warrant (or at least that the officer seeking the warrant honestly and reasonably believed those circumstances existed). That reasonableness must be '…more than idle wondering…some factual basis [must] exist…The facts must be sufficient to induce the suspicion in the mind of a reasonable person. The suspicion must be reasonable, as opposed to arbitrary, irrational or prejudiced' (*R v Bossley*, 2012).

To constitute a reasonable interference with privacy in the exercise of a hacking power, the factual basis for the application must be capable of satisfying the decision-maker that the alleged conduct is serious enough to warrant the vitiation of that privacy. That reasonableness must be satisfied in relation to both the nature of the alleged offences or threat to security, as well as the connection to the intelligence or information sought when the warrant is exercised. Equally, the Minister may only issue an ISA authorisation where he or she is satisfied that 'there are satisfactory arrangements in place to ensure that the nature and consequences of acts done in reliance on the authorisation will be reasonable' (ISA, s 9(1)(c)). ASIO also must abide by a standard of reasonableness when exercising powers which intrude on the privacy of others (Dutton, 2020, p. 3.4).

In all respects, we suggest that ISA agencies are essentially statutorily barred from undertaking activities with respect to Australian persons without satisfying the Minister of the reasonableness of such activities (ISA, ss 6(1), 6B(1) and 7(1)). This requirement invokes a need for proportionality, which may be met by reference to the need for the Minister to be satisfied in respect of an ISA authorisation that the target of the activities is involved in some serious contravention of national security, operational security, or Australian criminal law (ISA, s 9(1A)). This precludes the use of hacking powers under the ISA from use for trivial offences or for matters less than infringements upon Australia's national security.

That test for reasonableness sits alongside the one for necessity within section 9 of the ISA, as well as the exercise of assistance functions in section 13 of the ISA. Though this latter limitation is specifically carved out when ISA agencies cooperate either with ASIO or each other, ISA agencies cannot deviate from their core statutory functions while providing such assistance (even assuming they were specifically requested to do so). Similar tests are also present in the Defence Act, requiring the recognition of reasonableness in interfering in the privacy of persons affected by the exercise of powers under Part IIIAAA call-out orders (Defence Act, ss 39(2), 46(1)(b), 46(3), 51A(1), 51D(1), 51H(2), and 51N(1)(a)).

Proportionality

Finally, law enforcement and intelligence agencies carry an implicit requirement to ensure that their interference with privacy is proportionate; that is, it is the least invasive method or mechanism, considering the danger or threat being protected against. Serious crimes – such as terrorism – will warrant a more intrusive surveillance and data retention regime than would be the case with lesser offences (Aoláin, 2014, pp. 19–20).

Volume 12, Issue 1, 2024
ISSN: 2202-5677

The Comprehensive Review of the Legal Framework of the National Intelligence Community ("the Richardson Review") squarely confronted the idea of proportionality, noting that many of the intrusive powers exercised by intelligence agencies did not specifically incorporate the test of proportionality. The Richardson Review acknowledged that 'the exercise of extraordinary powers must be authorised by law and only limit individual rights to the extent that is reasonable, necessary and proportionate to the objective' (Richardson, 2019, p. 46). Indeed, the findings were that (Richardson, 2019, p. 37):

> While sharing highly-intrusive or sensitive intelligence may be reasonable, necessary and proportionate for purposes relevant to security (as defined in the ASIO Act) or the investigation of serious and organised crime, this is usually not the case for broader policy or regulatory purposes or the investigation of less serious offences.

In one of the few Australian cases to be heard before the Human Rights Committee of the UN, *Toonen* (1994) involved a challenge to Tasmanian laws which (at the time) made it a criminal offence to engage in acts of homosexuality, including between two consenting adults in private settings. In finding that the laws were not proportionate to the stated aim of 'public health and moral grounds', the Committee determined that 'criminalization of homosexual practices cannot be considered a reasonable means or proportionate measure to achieve the aim of preventing the spread of AIDS/HIV' (Toonen, 1994, p. 8.5).

There are examples in Australian case law. For example, in *SQH v Scott* (2022) an individual charged with several offences was the subject of a compulsory examination by the Crime and Corruption Commission. The individual refused to answer certain questions and appealed the attempt by the Commission to compel him to do so. In concluding that the examination was permitted, the Court considered the accused's right to privacy compared to whether there were other less restrictive ways to achieve the same goal, the nature of the crime, the protective measures in place to safeguard the rights of the individual, and the court's role in supervising the process (pp. 297–305). It concluded that the interference with the accused's rights was proportionate, but only because of the presence of safeguards including immunities and confidentiality (p. 306).

The ASIO Act, the SDA, and the ISA contain some similar safeguards for a potential suspect – though only by analogy. All three Acts contain penal provisions which outlaw the publication of information obtained by officers under the imprimatur of the various surveillance warrants listed in Part 2, whether falling within the scope of their respective duties or otherwise. Other criminal law provisions would also prevent the disclosure of information that carries a security classification (*Criminal Code* (Cth), ss 122.1-122.4A). All three Acts lack any reference to immunising the subject of information obtained incidental to a hacking power.

Collectively then, to be deemed an appropriate use of a hacking power that interferes with privacy, ASIO, the ISA, and SDA agencies should be satisfied with meeting an *implicit* test for proportionality, such as one expressed by McCrudden (2008). As the Richardson Review stated, '[u]sing such powers to answer basic intelligence questions would, in many cases, be

Volume 12, Issue 1, 2024
ISSN: 2202-5677

disproportionate' (Richarson, 2019, p. 63). The more intrusive the exercised power, the more safeguards are required to effectively achieve an appropriate balance (Hildebrandt, 2013, p. 359).

ASIO carries this explicit proportionality obligation, imposed by the Ministerial Guidelines, including 'any means used for obtaining and analysing information must be proportionate to the gravity of the threat posed and the likelihood of its occurrence' (Dutton, 2020). All the agencies which have mandatory Privacy Rules also carry an implicit obligation to consider the proportionality of their interference in the privacy of the subject of their hacking powers. Under the SDA, proportionality is essentially "baked-in" to the offences which are capable of substantiating applications for warrants, being 'relevant offences', those which are punishable by more than three years' imprisonment (SDA, s 6). For the ISA agencies, acts undertaken in accordance with Ministerial authorisations must be in accordance with the agency's functions, and not further than those functions (including the assistance functions). Finally, ASIO Act warrants may only be sought where the information collected would substantially assist intelligence collection related to 'security', which invokes some of the most serious threats known to Australian values, national interests, and civic society (ASIO Act, s 4).

CONCLUSION

We have presented the various legislative frameworks enabling law enforcement and intelligence agencies to break into the CDNs of suspects. These powers are incredibly intrusive and easily capable of constituting interferences in the privacy of those suspects, in circumstances where they are – consistent with the presumption of innocence – not guilty of a crime. It is, therefore, vitally important that the agencies vested with these powers are mindful of the appropriate considerations of their use. In response we therefore propose some moderate and meaningful law reform options which government could consider to address the shortfalls we have identified above.

The first requirement is to embed mindfulness of the privacy of affected individuals (including suspects) as a statutory footing. For example, the use of hacking powers by intelligence or law enforcement agencies (potentially as well as other intrusive powers for agencies protecting our national security) could be made subject to a requirement to consider whether other, less intrusive powers would be appropriate. Before 2019, the *Australian Crime Commission Act 2002* (Cth) – the legislation which created the Australian Crime Commission (now known as ACIC) – bestowed incredibly invasive compulsory powers on that agency. Individuals could be summonsed and forced to give evidence, even where that evidence could ultimately expose them to criminal charges. However, such powers could only be used once the Board of the Australian Crime Commission had issued a "special investigation determination",

Volume 12, Issue 1, 2024
ISSN: 2202-5677

which in turn required the Board to 'consider whether ordinary police methods of investigation into the matters are likely to be effective'.4

There are international examples of similar provisions. *The Investigatory Powers Act 2016* (UK) enables the UK's Government Communications Headquarters – the agency responsible for both overt and covert communications monitoring for national security purposes – to undertake targeted equipment interference activities specified in a warrant authorised by the Secretary of State. However, for such a warrant to be issued requires the Secretary of State be satisfied that the warrant is 'necessary to prevent and detect serious crime' and the conduct authorised by the warrant is 'proportionate to what is sought to be achieved by that conduct' (*Investigatory Powers Act 2016* (UK), s 102). A Judicial Commissioner reviews any such warrants granted in the UK and has broad powers to limit or annul warrants which are inappropriately issued. Such provisions could, with a minimum of amendment, be introduced in Australia.

In that vein, the degree to which any agency engages in assessments of necessity, reasonableness, and proportionality needs appropriate scrutiny to 'safeguard against abuse and the inadvertent or malicious disclosure of private information' (*El-Masri v the former Yugoslav Republic of Macedonia*, 2012). Such oversight can be conducted by a Board (as in the case of the ACIC), a committee (as in the case of ASIO) or a statutory agency or officer (such as the Independent National Security Legislation Monitor).

Australia already has such oversight bodies. Agencies bound by the ISA and SDA (as well as ASIO) are subject to robust scrutiny, both by the Inspector-General of Intelligence and Security (IGIS) as well as the Parliamentary Joint Committee on Intelligence and Security (PJCIS). However, to support the amendments we have proposed in law, these oversight bodies should also be empowered by their enabling statute to ensure that the actions of agencies under their purview accord with the requirements of necessity, reasonableness, and proportionality in the execution of their powers. This is especially necessary with respect to the hacking powers, which are more invasive than most other powers by an order of magnitude.

Finally, where intrusions into privacy have occurred without a proper reasonable or necessary basis, the aggrieved person/s should also have a right to seek redress or compensation. At the bare minimum, this must include a fulsome, independent, and transparent investigation to determine whether the agency has engaged in any impropriety or illegality (Housen-Couriel, 2022). Of course, this transparency can be difficult in the context of covert investigations by security and intelligence agencies; doubly so where the impugned interference in privacy involves the violation of a CDN by complex or controversial means.

What is required to have a meaningful pathway for redress compensation therefore is twofold. First, the often-impenetrable cloak of national security would need to be removed in

[4] *Australian Crime Commission Act 2002* (Cth) (as in force on 1 January 2003), s 7C(3). This provision was then removed by the *Australian Crime Commission Amendment (Special Operations and Special Investigations) Act 2019* (Cth), in favour of a broader 'public interest' test.

Volume 12, Issue 1, 2024
ISSN: 2202-5677

cases where a *prima facie* harm has been occasioned. Not only is this needed to ensure the investigation reaches conclusions or makes recommendations based on appropriate evidence, but also to prevent the misuse or abuse of national security confidentiality by the State. There has already been one case in Australia where concerns of national security were invoked improperly – or at least without a rational basis – involving the trial and imprisonment of a former intelligence officer for leaking classified information (Donaldson, 2022).

Second, the law should be amended to include a specific obligation for courts to consider whether – in an action of review or for damages – the agency involved complied with obligations of necessity, reasonableness, and proportionality (whether those obligations were imposed by the Privacy Rules or otherwise). In doing so, there may be a need for judicial willingness to expose at least some of the workings of our national security agencies to scrutiny to determine whether those principles were adhered to.

There remain challenges in balancing the human rights owed to individuals in a free, egalitarian, and democratic society, and the protection of that society from threats and harms to its interests – which can be volatile, unpredictable, and complex. Yet, that same exercise can no longer be resolved overwhelmingly in favour of national security agencies. Without properly ensuring respect for individual rights of privacy (alongside, one might argue, the other inalienable human rights flowing from Australia's ratification of international treaties), such agencies risk undermining the very values they set out to protect.

Volume 12, Issue 1, 2024
ISSN: 2202-5677

***About the authors*:**

Dr Brendan Walker-Munro is a Senior Research Fellow with the University of Queensland's Law School. Brendan's research focus is on aspects of national security law, particularly on the implications of national security risks on higher education research and teaching. He is also interested in the national security impacts of the law on topics such as privacy, identity crime and digital security.

Ruby Ioannou is a fourth-year law/arts Honours student at the University of Queensland, where she has also been working as a Research Assistant on a project funded by the UQ Cyber Seed Funding Grants. In 2021 she published a paper on the impact of COVID 19 on criminal law in Australia and a paper on the lawfulness of cyberattacks by Australian military and security agencies in in 2023. She has also worked as an intern and freelance educator.

Dr David Mount is a Lecturer in Cyber Criminology. Since 2019, has been working collaboratively with the Australian Federal Police on a series of research projects associated with the triaging of online child abuse material reports. David's research interests span law enforcement training regimes, information warfare, countering online child exploitation and the nexus of intelligence and law enforcement in the cyber realm.

Volume 12, Issue 1, 2024
ISSN: 2202-5677

REFERENCES

Beck. T., Senbet, L., & Simbanegavi, W. (2015*).* Financial Innovation and Innovation in Africa: An Overview. *Journal of African Economies, 24*(AERC Supplement1), i3–i11.

Anderson, Lord D. (2015). *A Question of Trust: Report of the Investigatory Powers Review*. Independent Reviewer of Terrorism Legislation.

Aoláin, F. N. (2014, September 23). *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and* Fundamental *Freedoms While Countering Terrorism*. UN Doc A/69/397. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/265/42/PDF/N1926542.pdf?OpenElement

Australian Criminal Intelligence Commission. (2020, August). *Information Handling Protocol*. ACIC. https://www.acic.gov.au/sites/default/files/2020-08/information_ handling_ protocol.pdf.

Australian Geospatial Intelligence Organisation. (2012, October 2). *Rules to Protect the Privacy of* Australians. AGO. https://www.igis.gov.au/sites/default/files/ago-privacy-rules.pdf.

Australian Secret Intelligence Service. (2021, November 30). *Rules to Protect the Privacy of Australians*. ASIS. https://www.asis.gov.au/Privacy-Rules/

Australian Signals Directorate. (2021, November 30). *Rules to Protect the Privacy of Australians*. ASD. https://www.asd.gov.au/publications/governance/rules-protect-privacy-australians/rules-protect-privacy-australians-2021

Austin, G. (2017, July 4). “Cyber revolution” in Australian Defence Force demands rethink of staff, training and policy. *The Conversation*. https://theconversation.com/cyber-revolution-in-australian-defence-force-demands-rethink-of-staff-training-and-policy-80317

Blumenthal, J. A., Adya, M., & Mogle, J. (2008). The multiple dimensions of privacy: Testing lay expectations of privacy. *University of Pennsylvania Journal of Constitutional Law, 11,* 331.

Bronitt, S. H., & Stellios, J. (2005). Telecommunications Interception in Australia: Recent Trends and Regulatory Prospects. *Telecommunications Policy, 29*(11), 875.

Corn, G. S. (2013). Terrorism, Tips, and the Touchstone of Reasonableness: Seeking a Balance Between Threat Response and Privacy Dilution. *Dickinson Law Review, 118,* 129.

De Hert, P., & Gutwirth, S. (2009). Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In S. Gutwirth, Y. Poullet, P. de Hert, C. de Terwangne & S. Nouwt (Eds.), *Reinventing Data Protection?* (pp. 3–44). Springer.

Volume 12, Issue 1, 2024
ISSN: 2202-5677

Defence Intelligence Organisation. (2023, June). *Rules to Protect the Privacy of Australians*. Department of Defence, Defence Intelligence Organisation. https://www.defence.gov.au/sites/default/files/2023-06/dio-privacyrules.pdf

Donaldson, G. (2022, June 17). *The operation of Part 3, Division 1 of the National Security Information (Criminal and Civil Proceedings) Act 2004 as it applies in the Alan Johns matter*. Independent National Security Legislation Monitor.

Dutton, P. (2020, August). *Minister's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its functions and the exercise of its powers*. Department of Home Affairs, ASIO. https://www.asio.gov.au/sites/default/files/Minister%27s%20Guidelines%20to%20the%20Australian%20Security%20Intelligence%20Organisation.pdf

Gray, A. (2021). The Australian Government's Use of the Military in an Emergency and the Constitution. *UNSW Law Journal, 44*(1), 357.

Hauch, J. M. (1994). Protecting Private Facts in France: The Warren & Brandeis Tort is Alive and Well and Flourishing in Paris. *Tulane Law Review, 8*, 1219–1274.

Hildebrandt, M. (2013). Balance or trade-off? Online security technologies and fundamental rights. *Philosophy & Technology, 26*, 357-379.

Hope, Justice R. (1977). *Royal Commission on Intelligence and Security: Fourth Report*. Commonwealth Printer.

Housen-Couriel, D. A. (2022). Managing Data Privacy Rights in Multilateral Coalition Operations' Information Sharing Platforms: A "Legal Interoperability" Approach. In R. Buchan & A. Lubin (Eds.), *The Rights to Privacy and Data Protection in Times of Armed Conflict.* NATO CCDCOE.

James, A. (2018). *Government mass surveillance and law in the five eyes countries* [Doctoral dissertation, University of Melbourne].

Letts, D., & McLaughlin, R. (2019). Military Aid to the Civil Power. In R. Creyke, D. Stephens & P. Sutherland (Eds.), *Military law in Australia* (pp. 117–128). Federation Press.

Lindsay, D. (2005). An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law. *Melbourne University Law Review, 29*(1), 131-178.

Lippis, Z. (2022). The *Defence Act 1903* (Cth): A guide for responding to Australia's large-scale domestic emergencies. *Melbourne University Law Review, 45*(2), 597-650.

Mann, M., Daly, A., Wilson, M., & Suzor, N. (2018). The limits of (digital) constitutionalism: Exploring the privacy-security (im) balance in Australia. *International Communication Gazette, 80*(4), 369.

Volume 12, Issue 1, 2024
ISSN: 2202-5677

Mayer-Schonberger, V., & Padova, Y. (2015). Regime change: enabling big data through Europe's new data protection regulation. *Columbia University Science & Technology Law Review, 17*, 315–335.

McCrudden, C. (2008). Human dignity and judicial interpretation of human rights. *European Journal of International Law, 19*(4), 655.

Moore, C. (2017). *Crown and Sword: Executive power and the use of force by the Australian Defence Force*. ANU Press.

Nowak, M. (1993). *United Nations Covenant on Civil and Political Rights: CCPR Commentary*. NP Engel.

Office of National Intelligence. (2022, September 22). *Rules to Protect the Privacy of Australians*. ONI. https://www.oni.gov.au/sites/default/files/documents/2022-10/ONI%20Privacy%20Rules%20-%20As%20from%201%20October% 202022.pdf

Richardson, D. (2019, December). *Comprehensive Review of the Legal Framework of the National Intelligence Community: Final Report*. Attorney-General's Department.

Slobogin, C., & Schumacher, J. E. (1993). Rating the Intrusiveness of Law Enforcement Searches and Seizures. *Law & Human Behaviour, 17*(1), 183.

Strossen, N. (1990). Recent US and International Judicial Protection of Individual Rights: A Comparative Legal Process Analysis and Proposed Synthesis. *Hastings Law Journal, 41*, 805–904.

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review, 4*, 193–206.

Willoughby, A. (2017). Biometric surveillance and the right to privacy [commentary]. *IEEE Technology & Society Magazine, 36*(3), 41-45.

Witzleb, N. (2020). Another Push for an Australian Privacy Tort – Context, Evaluation and Prospects. *Australian Law Journal, 94*, 765–782.

LEGISLATION AND CASES

Airey v Ireland (European Court of Human Rights, Application No. 6289/73, Judgement of 9 October 1979).

American Convention on Human Rights, 1144 UNTS 123 (opened for signature 22 November 1969, entered into force 18 July 1978).

Arab Charter on Human Rights, 12 IHRR 893 (adopted 22 May 2004, entered into force 15 March 2008).

Volume 12, Issue 1, 2024
ISSN: 2202-5677

Australian Crime Commission Act 2002 (Cth).

Burmah Oil Co Ltd v Lord Advocate [1965] AC 75.

Convention on the Rights of the Child, 1577 UNTS 3 (opened for signature 20 November 1989, entered into force 2 September 1990).

Criminal Code (Cth).

Cyprus v Turkey (2001) 35 EHRR 731.

El-Masri v the former Yugoslav Republic of Macedonia, App no 39630/09 (ECtHR, 13 December 2012).

Entick v Carrington [1765] EWHC KB J98.

European Convention for the Protection of Human Rights and Fundamental Freedoms, ETS 5 (opened for signature 4 November 1950, entered into force 3 September 1953).

International Covenant on Civil and Political Rights, 999 UNTS 171 (opened for signature 16 December 1966, entered into force 23 March 1976).

International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (GA Res 158, UN GAOR, 45 Sess, UN Doc A/RES/45/158).

International Convention on the Rights of Persons with Disabilities, 2515 UNTS 3 (adopted 24 January 2007, entered into force 3 May 2008).

Investigatory Powers Act 2016 (UK).

Klass & Ors v Germany (1979) 2 EHRR 214.

Leander v Sweden App no 9248/81 (1987, ECtHR) 48.

Minister for Immigration and Ethnic Affairs v Ah Hin Teoh (1995) 183 CLR 273.

Minister for Immigration and Border Protection v SZVFW (2018) 92 ALJR 713.

R v Bossley [2012] QSC 292.

R v N [2015] QSC 91.

R v Peirson [2014] QSC 134.

R v Secretary of State for the Home Department; Ex parte Northumbria Police Authority [1989] 1 QB 26.

SQH v Scott [2022] 10 QR 215.

Szabo v Vissy Hungary, App no 37138/14 (12 January 2016).

Volume 12, Issue 1, 2024
ISSN: 2202-5677

Universal Declaration of Human Rights (GA Res 217A (III), UN GAOR, UN Doc A/810, 10 December 1948).

Toonen v Australia, No 488/1992, UN Doc CCPR/C/50/D/488/1992 (31 March 1994).

X v Iceland (1976) 5 DR 86.