Cambridge Law Journal, **83(1)**, March 2024, pp. 62–98
doi:10.1017/S0008197323000466

ESPIONAGE LAW IN THE UK AND AUSTRALIA: BALANCING EFFECTIVENESS AND APPROPRIATENESS

SARAH KENDALL*

ABSTRACT. *This article engages in a comparative analysis of espionage law in the UK and Australia to determine whether the laws in each country are effective and appropriate. It finds that, while the espionage laws in both countries are largely capable of effectively addressing modern espionage, this has come at the expense of appropriateness – specifically, aspects of the laws in both jurisdictions are complex, uncertain and overly broad, and defences and other safeguards for legitimate conduct have limitations. The article argues that, while the effectiveness of espionage (and other national security) laws is an important consideration, this must be balanced with appropriateness to ensure that core rule of law values and legal principles are not undermined.*

KEYWORDS: *spying*; *intelligence*; *cyberespionage*; *foreign interference*; *national security*; *comparative law*; *law reform*; *rule of law.*

I. INTRODUCTION

After extensive consultations, in July 2023 the UK's Parliament passed the National Security Act 2023, which introduced sweeping reforms to counter-state threats laws. These included the overhaul of espionage[1] and sabotage offences,[2] the introduction of novel offences for foreign interference,[3] the creation of prevention and investigation measures for individuals believed to be involved in foreign power threat activity[4] and the introduction of the Foreign Influence Registration Scheme (which requires registration of "foreign activity arrangements").[5] Introducing the first significant reforms to counter-state threats legislation since 1939,[6]

*School of Law, The University of Queensland. Address for Correspondence: s.kendall@uq.net.au. I would like to thank Associate Professor Rebecca Ananian-Welsh and the anonymous reviewers for their invaluable comments on earlier drafts.

[1] National Security Act 2023, ss. 1, 2.
[2] Ibid., s. 12. Previously, there was no standalone offence for sabotage, but rather the espionage offences were held to encompass sabotage: *Chandler v Director of Public Prosecutions* [1964] A.C. 763 (H.L.).
[3] National Security Act 2023, ss. 13, 16.
[4] Ibid., pt. 2.
[5] Ibid., pt. 4.
[6] Previous counter-state threats laws were found in the Official Secrets Acts 1911, 1920 and 1939. The Official Secrets Act 1989 deals with unauthorised disclosures of classes of information.

the National Security Act was said to be necessary because the threat of foreign hostile activity against the UK's interests had evolved since the early 1900s and was growing.[7]

Just five years earlier, Australia also reformed its counter-state threats laws. Specifically, it modernised its national security laws (including espionage, sabotage and secrecy offences) and introduced unprecedented foreign interference offences,[8] as well as the Foreign Influence Transparency Scheme.[9] These reforms were said to be necessary to modernise the law so that it could better address the threat posed by today's foreign actors, including those seeking to interfere with Australian democratic processes or to access critical information on Australia and its allies.[10]

This article focuses on just one aspect of the national security reforms introduced in the UK and Australia – espionage offences. It engages in a comparative analysis of those laws to determine whether the laws in each country are effective and appropriate, using this analysis to emphasise the importance of laws that balance effectiveness with appropriateness.

Espionage against the UK and Australia is a growing national security threat that has – at least in Australia – outstripped the threat of terrorism.[11] In July 2020, the UK's Intelligence and Security Committee published its *Russia* report, which concluded that Russia currently poses a "significant threat to the UK on a number of fronts – from espionage to interference in democratic processes".[12] Just two months later, the Law Commission released its *Protection of Official Data Report* which found that, because of developments in technology, "the threat of espionage … is of a wholly different order than was the case even twenty years ago".[13] In February 2023, Mike Burgess, Director-General of the Australian Security Intelligence Organisation (ASIO), described espionage and foreign interference as an "unprecedented challenge" and ASIO's "principal security concern".[14] He warned that "more Australians are being targeted for espionage and foreign interference than at any time in Australia's history".[15]

[7] Explanatory Notes, National Security Bill 2022, [1]–[7].
[8] Criminal Code 1995 (Cth) ("Criminal Code"), sched. 1, divs. 82, 91, 92, 92A, 122.
[9] Foreign Influence Transparency Scheme Act 2018 (Cth).
[10] Revised Explanatory Memorandum, National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (Cth), 2–4; Commonwealth, *Parliamentary Debates*, House of Representatives, 26 June 2018, 1, 10. From 2018 to 2021, foreign interference attempts have occurred "against all levels of Australian politics, and in every single state and territory": Australian Security Intelligence Organisation (ASIO), "Director-General's Annual Threat Assessment", available at https://www.asio.gov.au/publications/speeches-and-statements/director-generals-annual-threat-assessment-2021.html (last accessed 1 November 2023).
[11] ASIO, *Annual Report: 2021–22* (Canberra 2022), 4.
[12] Intelligence and Security Committee, *Russia*, HC 632 (London 2020), 19.
[13] Law Commission, *Protection of Official Data Report*, HC 716 (London 2020), 1.
[14] ASIO, "Annual Threat Assessment".
[15] Ibid.

Due to the growing nature of the threat, it is imperative that today's espionage laws are effective in terms of being capable of achieving their intended aim. The objective aim of espionage laws is to address modern espionage (although some governments may arguably have ulterior motives, such as silencing whistleblowers or protestors). Modern espionage generally involves the use of technology and the internet (cyberespionage) by foreign powers (even allies) to collect, store and communicate a range of valuable information, such as military, trade secret and scientific information.

Academics have argued that Australia's new 2018 espionage offences are capable of effectively addressing modern espionage.[16] Therefore, Australia's offences may usefully be compared with the UK's new 2023 espionage laws to determine whether those laws are also capable of effectively addressing the threat. However, Australia's espionage offences have also been criticised for being uncertain and overly broad.[17] While this may be what legislators intended, because such laws give law enforcement and intelligence agencies greater powers and flexibility to investigate and prosecute alleged espionage (especially as the nature of espionage may change over time), such laws are not appropriate criminal laws. In particular, laws that are broad and lack clarity have the capacity to capture conduct that should not be criminalised – in the espionage context, for example, the conduct of journalists, whistleblowers, academics and researchers.

Although the concerns above have not yet played out in Australia, Australian whistleblowers and journalists have been investigated and, in some instances, prosecuted for other national security offences. For example, Witness K, a former Australian Secret Intelligence Service (ASIS) agent, and his security cleared lawyer, Bernard Collaery, were charged with secrecy offences for revealing that ASIS allegedly bugged the offices of the East Timorese Cabinet during treaty negotiations. Military lawyer David McBride compiled a report on alleged war crimes committed by Australian soldiers in Afghanistan, which he leaked to the Australian Broadcasting Corporation (ABC). He was charged with several offences, including unlawfully disclosing a Commonwealth document and theft of Commonwealth property.

In 2019, News Corp journalist Annika Smethurst's home was raided by the Australian Federal Police (AFP) after she published stories on proposed new domestic surveillance powers for the Australian Signals Directorate (ASD). These stories were based on a top-secret departmental memo and,

[16] E.g. S. Kendall, "Australia's New Espionage Laws: Another Case of Hyper-Legislation and Over-Criminalisation" (2019) 38 University of Queensland Law Journal 125.

[17] Ibid. See also R. Ananian-Welsh, S. Kendall and R. Murray, "Risk and Uncertainty in Public Interest Journalism: The Impact of Espionage Law on Press Freedom" (2021) 44 Melbourne University Law Review 764; S. Kendall, "The Erosion of Academic Freedom: How Australian Espionage Law Impacts Higher Education and Research" (2022) 44 Sydney Law Review 503; R. Ananian-Welsh and S. Kendall, "Crimes of Communication: The Implications of Australian Espionage Law for Global Media" (2022) 27 Communication Law and Policy 3.

while her conduct appeared to contravene secrecy offences, she was not charged. Just 24 hours later, the AFP raided the Sydney headquarters of the ABC in relation to a report, the "Afghan Files", published by investigative journalists Dan Oakes and Sam Clarke. This report was based on secret defence force documents and revealed that Australian military personnel had committed severe human rights violations in Afghanistan. Oakes and Clarke were informed that they were under investigation for offences, including unlawfully obtaining information regarding Australia's defence capabilities, receiving "prescribed" information and receipt of stolen goods, but they have not been charged. While Smethurst, Oakes and Clarke have avoided prosecution to date, the AFP has warned that it will continue to pursue cases like these because they involve a serious breach of national security.[18]

While the examples above did not involve espionage offences, the conduct of those involved certainly could have constituted espionage under Australian law, and similar conduct in the future could result in charges of espionage.[19] This highlights the importance of laws that are not just effective, but are also *appropriate*. Appropriateness can encompass a range of considerations,[20] but relevant to this article are two considerations that reflect rule of law values and principles: (1) the clarity of the laws; and (2) whether the laws are appropriate in scope. Espionage laws that are unclear and/or overly broad may be effective but run the risk of being used to punish (or silence) legitimate conduct, such as whistleblowing.

Laws in the UK and Australia have been chosen for analysis because both countries have similar legal, political and cultural traditions, including strong respect for the rule of law. Furthermore, Australia frequently looks to the UK when conducting official inquiries and reviews[21] and has modelled some of its national security laws and policies on those found in the UK.[22] The UK has borrowed some aspects of Australia's national security laws too[23] and has looked to Australian law for guidance when

[18] Press Conference with Ian Mcartney, *ABC News*: Video, "AFP Says They Will Continue to Pursue Cases Like That of Annika Smethurst", available at https://www.abc.net.au/news/2020-05-27/afp-says-they-will-continue-to-pursue-cases-like/12292164?nw=0 (last accessed 1 November 2023). For in-depth discussion of these (and other) examples, see R. Ananian-Welsh, R. Cronin and P. Greste, "In the Public Interest: Protections and Risks in Whistleblowing to the Media" (2021) 44 University of New South Wales Law Journal 1242.

[19] Ananian-Welsh, Kendall and Murray, "Risk and Uncertainty".

[20] Effectiveness and appropriateness are discussed in T. Legrand and T. Elliott, "A New Preventive Justice Framework for Assessing Counter-Terrorism Law and Policy" in T. Tulich, R. Ananian-Welsh, S. Bronitt and S. Murray (eds.), *Regulating Preventive Justice: Principle, Policy and Paradox* (New York 2017).

[21] A.W. Neal, "The Parliamentarisation of Security in the UK and Australia" (2021) 74 Parliamentary Affairs 464, 467.

[22] E.g. Australia's counter-terrorism law and policy were copied "especially [from] the United Kingdom": G. Williams, "A Decade of Australian Anti-Terror Laws" (2011) 35 Melbourne University Law Review 1136, 1171. Additionally, Australia modelled its "first-generation" espionage offences (introduced in 1914) on the offences that existed in the UK at the time.

[23] Neal, "Parliamentarisation of Security", 467.

determining how to reform its counter-state threats legislation.[24] Additionally, useful comparisons can be made between legal frameworks that have both been introduced to tackle the same threat.

A final reason why the UK and Australia have been chosen for analysis is that both countries are members of the "Five Eyes" Intelligence Alliance. While this alliance requires the UK, Australia, US, Canada and New Zealand to share intelligence information, Julian Assange/WikiLeaks and Edward Snowden revealed that the global surveillance network was being used (at least by the US) to monitor domestic citizens and close allies, and to engage in industrial espionage.[25] Their leaks sparked global concern over citizens' privacy rights and highlighted once again the asymmetrical nature of the alliance, with the US setting the agenda.[26] Steps towards strengthening espionage laws in the UK and Australia could therefore be at the behest of the US – so as to expand the scope of information the US has access to. However, it could also be a sign of rising geopolitical tensions between the Five Eyes and nations such as China and Russia, and of the potential lead up to war.[27] Regardless of the political nuances surrounding *why* Australia and the UK have reformed their espionage laws, the Five Eyes *do* ultimately place espionage (and the legal response to espionage) at the centre of their dealings. A comparative analysis of espionage laws in two of the Five Eyes nations is therefore apt.

This article begins, in Part II, with an overview of "modern espionage". This is followed, in Part III, with a discussion of the UK's 2023 espionage laws and how they could be applied in practice. This discussion draws on analysis of the UK's previous espionage offences and how those offences were applied in practice. Part IV provides an overview of Australia's 2018 espionage offences, giving examples of how they could apply to real-world scenarios. Part V then compares and contrasts the laws in the two jurisdictions, analysing whether they are capable of effectively meeting the threat of modern espionage. A similar approach is taken in Part VI, which assesses whether the laws are appropriate in terms of their clarity and scope.

II. What Is Modern Espionage?

MI5 describes espionage as "the process of obtaining information that is not normally publicly available, using human sources (agents) or technical

[24] E.g. HC Deb. vol. 720 cols. 351–52, 382 (18 October 2022).
[25] P.F. Walsh and S. Miller, "Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden" (2016) 31 Intelligence and National Security 345.
[26] A. O'Neil, "Australia and the 'Five Eyes' Intelligence Network: The Perils of an Asymmetric Alliance" (2017) 71 Australian Journal of International Affairs 529, 529.
[27] A. Greene, "Home Affairs Secretary Mike Pezzullo Warns 'Drums of War' Are Beating in a Message to Staff", *ABC News*, available at https://www.abc.net.au/news/2021-04-26/mike-pezzullo-home-affairs-war-defence-force/100096418 (last accessed 26 April 2020).

means (like hacking into computer systems)".[28] While espionage traditionally involved spies going undercover in the field to collect information and documents, as technology advanced following the World Wars, espionage has increasingly been conducted using technology and the Internet – that is, cyberespionage has become the norm. Cyberespionage allows a person – located anywhere in the world – to collect and disseminate a vast array of data in a matter of seconds (as occurred, for example, with the leaks by Assange and Snowden).[29]

While wartime espionage largely focused on the theft of military and scientific secrets by "enemy" countries, modern espionage targets a much wider range of information and can be conducted by *any* state (or their entities), including allies. Any type of valuable information is collected, including military, defence, political, diplomatic, economic, corporate, technological, critical infrastructure and natural resource information, as well as information on (or samples of) intellectual property, scientific discoveries (such as a new vaccine) and research findings. Therefore, not only have there been significant changes to how information is collected and communicated, but also the scope of information that is targeted – and by whom it is targeted – have broadened incredibly since the World Wars when espionage laws in the UK and Australia were originally enacted.[30]

III. Espionage Laws in the UK

The UK's first espionage offences, introduced in 1889,[31] were significantly amended in 1911.[32] These reforms, introduced in the context of pre-World War I (WWI) tensions, were said to be necessary to "strengthen the law for dealing with … espionage generally".[33] Further (minor) amendments were made in 1920,[34] on the basis that the 1911 laws inadequately captured "modern spying".[35]

Section 1(1) of the Official Secrets Act 1911 provided that it was a felony punishable by up to 14 years' imprisonment for "any person for any purpose prejudicial to the safety or interest of the State" to:

[28] MI5, "Counter-Espionage", available at https://www.mi5.gov.uk/counter-espionage (last accessed 26 May 2023).
[29] D. Pun, "Rethinking Espionage in the Modern Era" (2017) 18 Chicago Journal of International Law 353, 357–58; S. Mohanty, "Cyber Espionage – Burglary of the 21st Century" (2017) 109 Intellectual Property Forum: Journal of the Intellectual and Industrial Property Society of Australia and New Zealand 51, 52.
[30] For in-depth discussion of historical and modern espionage practices, see Kendall, "Australia's New Espionage Laws", 128–34.
[31] Official Secrets Act 1889.
[32] Official Secrets Act 1911.
[33] HL Deb. vol. 9 cols. 641–42 (5 July 1911).
[34] Official Secrets Act 1920. Minor amendments were also made in 1939: Official Secrets Act 1939.
[35] HC Deb. vol. 135 cols. 1537–38 (2 December 1920).

(1) Approach, inspect, pass over, be "in the neighbourhood of, or enter[] any prohibited place"[36] ("Espionage by Trespass");
(2) Make any "sketch, plan, model or note which is calculated to be or might be or is intended to be directly or indirectly useful to an enemy"[37] ("Espionage by Information Gathering"); or
(3) Obtain, collect, record, publish or communicate "to another person any secret official code word, … pass word, … sketch, plan, model, article, note, or other document or information which is calculated to be or might be or is intended to be directly or indirectly useful to an enemy"[38] ("Espionage by Information Communication").

In addition to these three offences, section 7 of the Officials Secrets Act 1920 criminalised the inchoate offences of attempts, solicitation or incitement, aiding or abetting and acts done in preparation for the espionage offences ("Inchoate Espionage Offences"). Some of these inchoate offences (such as attempts and acts done in preparation) can be considered "pre-crimes". Pre-crimes essentially punish people for crimes that may occur in the future, not retrospectively for substantive crimes that have already been committed.

A. The 2023 Offences

The espionage offence framework under the Official Secrets Acts was heavily criticised by the Intelligence and Security Committee in 2020 for being out of date and "not fit for purpose".[39] To rectify this, the framework was entirely overhauled in 2023. The new offences introduced by the National Security Act were argued to be necessary to "reflect the evolving threat and the interconnected nature of the modern world" by capturing "modern methods of spying".[40] To that end, the Act introduced three new espionage offences: "Protected Information Espionage"; "Trade Secrets Espionage"; and a preparatory offence.[41] No express defences were introduced. The three espionage offences will be explained further below. This will be followed in the next section by a discussion of their key terms and elements.

[36] Official Secrets Act 1911, s. 1(1)(a).
[37] Ibid., s. 1(1)(b).
[38] Ibid., s. 1(1)(c).
[39] Intelligence and Security Committee, *Russia*, 34.
[40] Explanatory Notes, National Security Bill 2022, [14].
[41] The National Security Act 2023 also includes an offence of "assisting a foreign intelligence service", which criminalises engaging in any conduct intended to (or known to be likely to) "materially assist a foreign intelligence service in carrying out UK-related activities": section 3. Australia introduced similar offences of "supporting" or "funding" a foreign intelligence agency in 2018: Criminal Code, ss. 92.7, 92.8, 92.9, 92.10. However, Australia has classified these offences as "foreign interference" offences and, for that reason, the UK's section 3 offence will not be analysed in this article.

Protected Information Espionage makes it an offence (punishable by up to life in prison) to obtain, copy, record, retain, disclose or provide access to protected information where the person's conduct is "for a purpose that they know, or having regard to other matters known to them ought reasonably to know, is prejudicial to the safety or interests of the United Kingdom".[42] The "foreign power condition" must also be met in relation to the person's conduct. This offence essentially replaces the 1911 Act's Espionage by Information Gathering and Espionage by Information Communication offences.[43]

Trade Secrets Espionage criminalises similar conduct. It makes it an offence punishable by up to 14 years' imprisonment to obtain, copy, record, retain, disclose or provide access to a trade secret without authorisation where the person "knows, or having regard to other matters known to them ought reasonably to know, that their conduct is unauthorised".[44] Reflecting the character of the offence as a counter-state threats offence, Trade Secrets Espionage also requires the foreign power condition to be met. No equivalent of this offence was found in the Official Secrets Acts.

The National Security Act also introduced a preparatory offence that applies to several "underlying" offences found in the Act, including Protected Information and Trade Secrets Espionage.[45] The preparatory offence provides that a person commits a crime punishable by up to life in prison if, with the intention of committing acts constituting one of the espionage offences or with the intention of such acts being committed by another person, the person "engages in any conduct in preparation for the commission of such acts".[46] To be found guilty of the offence, it is not necessary that the person have in mind specific acts constituting an espionage offence, nor is it necessary that an espionage offence subsequently be committed.[47] This offence is a broad offence that essentially captures "any conduct" and, therefore, is primarily limited by its fault element (an intention to commit an espionage offence).

The preparatory offence was the only one of the 1920 Inchoate Espionage Offences to be included in the National Security Act; the other offences were omitted because they are already found in common law and/or statute (and, therefore, they can be attached to any of the underlying espionage offences to create pre-crimes, such as soliciting espionage).[48] However, because the

[42] National Security Act 2023, s. 1(1)(b).
[43] The National Security Act 2023 includes two offences that are intended to replace the 1911 Act's Espionage by Trespass offence: sections 4, 5. However, these offences were – appropriately – not classified as espionage offences under the Act.
[44] Ibid., s. 2(1)(c).
[45] Ibid., s. 18(3).
[46] Ibid., ss. 18(1), 18(6).
[47] Ibid., s. 18(2); Explanatory Notes, National Security Bill 2022, [130]–[131].
[48] Explanatory Notes, National Security Bill 2022, [39]. E.g. Criminal Attempts Act 1981; Serious Crime Act 2007.

preparatory offence is now a substantive offence under the Act, those inchoate offences also have the capacity to attach to the preparatory offence. This could create "pre-pre-crimes" (such as soliciting someone to prepare for espionage or attempting to prepare for espionage) which further broaden the scope of the law by criminalising conduct a further step removed from the commission of any substantive offence. These offences therefore significantly expand the scope of the UK's 2023 espionage framework.

The three new espionage offences have a wider territorial ambit than the 1911 and 1920 Acts' offences (which only applied to acts committed in "any part of His Majesty's dominions" or, if committed abroad, only when committed by British Officers or subjects[49]). Specifically, all three offences apply to conduct that occurs within or outside the UK,[50] regardless of the individual's nationality.[51] However, if conduct constituting Trade Secrets Espionage takes place wholly outside the UK, to be an offence the trade secret must have been in the possession or under the control of a "UK person" (i.e. a UK national or resident).[52] The wider territorial ambit of the 2023 Act's offences has the effect that espionage committed outside the UK by foreign citizens – as frequently occurs in cyberespionage – is criminalised.

B. Key Terms and Elements

Unlike previous espionage offences (where the scope of most key terms was left to the courts), many of the terms and elements of Protected Information and Trade Secrets Espionage have been defined in legislation. For example, the National Security Act defines both "protected information" and "trade secret" – the type of information that is the subject of these two offences. Both terms refer to "any information, document or other article" (for simplicity, this article will use "information" to refer to this phrase).[53] To be protected information, access to such information must be "restricted in any way" or it must be reasonable to expect that access to such information would be so restricted, for the purpose of protecting "the safety or interests of the United Kingdom".[54] "Trade secret" is also comprehensively defined, essentially encompassing commercially valuable information that is not generally known by experts in the field and whose value would be adversely affected if it became generally known.[55]

[49] Official Secrets Act 1911, s. 10(1).
[50] National Security Act 2023, ss. 1(3), 2(4), 18(5).
[51] Ibid., s. 36(1)(a).
[52] Ibid., ss. 2(5)–(7).
[53] Ibid., ss. 1(2), 2(2).
[54] Ibid., s. 1(2).
[55] Ibid., s. 2(2).

https://doi.org/10.1017/S0008197323000466 Published online by Cambridge University Press

Although the National Security Act provides guidance as to what constitutes protected information and trade secrets, it does not further explain what "information, document or other article" encompasses, except that "information" includes "information about tactics, techniques and procedures".[56] While these terms could extend to digital information (as is targeted by cyberespionage), it is less clear whether they include things such as samples and prototypes (for example, a sample of a new vaccine or a prototype of sonic weaponry).

Central to both Protected Information and Trade Secrets Espionage is the "foreign power condition". That condition will be met if the conduct (or course of conduct of which it forms a part[57]) is "carried out for or on behalf of a foreign power" and the person "knows, or having regard to other matters known to them ought reasonably to know", that that is the case.[58] The National Security Act provides that conduct or a course of conduct "is in particular to be treated as carried out for or on behalf of a foreign power" if it is instigated, directed or controlled by, "carried out with financial or other assistance provided by", or "carried out in collaboration with, or with the agreement of, a foreign power".[59] This element can be satisfied by a "direct or indirect relationship" between the conduct and the foreign power ("for example, there may be an indirect relationship through one or more companies").[60] Additionally, where the conduct in question is the person's conduct (and not a course of conduct), the foreign power condition can be met if "the person intends the conduct in question to benefit a foreign power"[61] (although it is "not necessary to identify a particular foreign power"[62]).

The National Security Act provides a comprehensive definition of "foreign power".[63] Specifically, a foreign power includes the sovereign or head of a foreign state;[64] a foreign government (or part of one);[65] "an agency or authority of a foreign government"[66] or one "responsible for administering the affairs of an area within a foreign country";[67] or "a governing political party of a foreign government".[68] A "government" is not restricted to the government itself, but "includes persons exercising the functions of a

[56] Ibid., s. 34(1).
[57] By the person alone, or the person and others: ibid., s. 31(4).
[58] Ibid., s. 31(1).
[59] Ibid., s. 31(2).
[60] Ibid., s. 31(3).
[61] Ibid., s. 31(5)
[62] Ibid., s. 31(6).
[63] Ibid., s. 32(1).
[64] Ibid., s. 32(1)(a).
[65] Ibid., s. 32(1)(b).
[66] Ibid., s. 32(1)(c).
[67] Ibid., s. 32(1)(d).
[68] Ibid., s. 32(1)(e). A "governing political party" is one where persons hold "political or official posts in the foreign government": (1) as a result of their membership in the party; or (2) where they are "subject to the direction or control of" the party in exercising the functions of their posts: ibid., s. 32(2).

government".[69] This definition of foreign power makes it clear that *any* foreign power could fall within its scope (including allies) and not just "enemies" as was used in previous espionage offences.

In addition to the foreign power condition, a second term is fundamental to Protected Information Espionage: "safety or interests of the UK". That term is incorporated as a fault element of the offence ("for a purpose that … is prejudicial to the safety or interests of the United Kingdom"[70]) as well as an element of "protected information".[71] Despite its importance, however, the term has not been defined in legislation. It was also not defined in the Official Secrets Act 1911, where the term formed part of the fault element of the previous espionage offences ("for any purpose prejudicial to the safety or interests of the State"[72]).

While it was not defined in the Official Secrets Act 1911, "safety or interests of the State" has been judicially considered. In *Chandler v DPP*, the court held that the "State" encompasses the organs of government of a national community,[73] with "safety or interests of the State" referring to the objects of State policy determined by the Crown on the advice of Ministers.[74] Similarly, in *Secretary of State for the Home Department v Rehman*, the court held that:

> whether something is "in the interests" of national security is not a question of law. It is a matter of judgment and policy. Under the constitution of the United Kingdom and most other countries, decisions as to whether something is or is not in the interests of national security are not a matter for judicial decision. They are entrusted to the executive.[75]

Although the National Security Act uses the UK instead of "State" or "national security", drawing on the reasoning in *Chandler* and *Rehman*, "safety or interests of the UK" could be interpreted to mean the objects of UK government policy determined by the Crown on the advice of Ministers.

The court in *Chandler* also considered the scope of the fault element of previous espionage offences — "for any purpose prejudicial to the safety or interests of the State". Specifically, the court held that this fault element consisted of both a subjective and an objective component – the defendant's "purpose" was determined subjectively, but whether this subjective purpose prejudiced the safety or interests of the State was

[69] Ibid., s. 32(4).
[70] Ibid., s. 1(1)(b).
[71] Ibid., s. 1(2).
[72] Official Secrets Act 1911, s. 1(1).
[73] *Chandler v DPP* [1964] A.C. 763, 807 (Lord Devlin).
[74] Ibid., at 813 (Lord Pearce).
[75] *Secretary of State for the Home Department v Rehman* [2001] UKHL 47, [2003] 1 A.C. 153, at [50] (Lord Hoffmann). In that case, the court held that "national security" means "the security of the United Kingdom and its people", at [50]. This term has not been used in the espionage offences contained in the National Security Act 2023.

determined objectively. Therefore, it was irrelevant whether the defendant thought that his or her purpose was prejudicial or beneficial.

The scope of this fault element was criticised by the Law Commission, which emphasised that the reason for the person's conduct is what is important.[76] To remedy this problem, the fault element of Protected Information Espionage is entirely subjective. Specifically, the person's conduct must have been "for a purpose that they know, or having regard to other matters known to them ought reasonably to know, is prejudicial to the safety or interests of the United Kingdom".[77] A similar fault element has been included in Trade Secrets Espionage (in relation to whether the conduct is unauthorised[78]) as well as in the foreign power condition (in relation to whether the conduct was "for or on behalf of a foreign power"[79]).

C. Application of the UK's Espionage Laws

Many convictions were secured under the UK's previous espionage offences; so, there were many reported cases from which application of the laws could be assessed. Most cases on Espionage by Information Gathering or Communication involved UK military or intelligence members or employees of UK government agencies who passed highly sensitive information to foreign officials or agents.[80] These foreign officials were citizens of countries with whom the UK was or had been at war (for example, Russia and Germany); so, they were clearly enemies. The cases on preparing for espionage involved similar circumstances.[81] All of these prosecutions were successful, with defendants sentenced to lengthy periods of imprisonment (seven to 42 years' imprisonment for espionage offences and two to two-and-a-half years' for preparatory offences).

However, none of these cases involved information collected from outside the UK by foreign citizens (from countries that were not clearly "enemies") using modern espionage methods, such as cyber hacking. Nor did any involve information other than defence or military information, such as trade secrets, which may be just as damaging to the UK if it were obtained by a foreign power. Such conduct is typical of modern espionage, yet was not criminalised under the UK's previous espionage laws. The 2023 offences are intended to rectify these issues.

[76] Law Commission, *Protection of Official Data*, 33–35.
[77] National Security Act 2023, s. 1(1)(b).
[78] Ibid., s. 2(1)(c).
[79] Ibid., s. 31(1)(a).
[80] E.g. *R. v James* [2009] EWCA Crim 1261, [2010] 1 Cr. App. R. (S.) 57; *R. v Smith* [1996] 1 Cr. App. R. (S.) 202; *R. v Prime* (1983) 5 Cr. App. R. (S.) 127; *R. v Prager* [1972] 1 W.L.R. 260 (C.A.); *R. v Britten* [1969] 1 W.L.R. 151 (C.A.); *R. v Blake* [1962] 2 Q.B. 377; *R. v AB* [1941] 1 K.B. 454.
[81] *R. v Bingham* [1973] Q.B. 870; *R. v Oakes* [1959] 2 Q.B. 350.

The espionage offences under the National Security Act apply to a broader scope of information than did the previous offences – specifically, trade secrets as well as any information that is "restricted in any way" for the purpose of protecting the safety of interests of the UK (whether in physical or digital form). However, while this latter category could encompass top-secret defence and military information, as well as other sensitive information (such as political, diplomatic, critical infrastructure, economic and scientific information), the bounds of this category are set not by the nature of the information itself, but by government decisions regarding how it should be handled.

On the role of government decisions consider, for example, the UK's three security classifications for information that determine the necessary level of protection (or restriction) – Official, Secret and Top Secret.[82] According to the UK Government, "All information that is created or processed by organisations subject to the [Government Security Classification Policy] is OFFICIAL by default ... The majority of government information is classified as OFFICIAL" – the "OFFICIAL tier contains a huge volume of information".[83] Such information must be securely handled and should generally be marked as "OFFICIAL", although this requirement can be overidden by organisational policy.[84] Clearly, Official information could encompass a range of information that is technically restricted but is not truly sensitive or would not pose a tangible threat to the UK's safety or interests. That it could do so significantly broadens the scope of the 2023 espionage laws.

In addition to applying to a broader scope of information than did the previous offences, as discussed above, the 2023 offences apply to a wide range of foreign actors. They also apply beyond the UK to conduct that takes place outside the UK too. Collectively, the 2023 reforms mean that the new espionage offences have the capacity to capture the actions of any foreign spy who might use more modern methods of spying (such as cyberespionage) to access a range of sensitive information that might harm the UK if it were to be obtained.

However, although these laws have the capacity to criminalise conduct that clearly constitutes modern espionage, they are also broad enough to capture some situations which may not involve genuine spying. For example, the "foreign power condition" has been defined such that it may apply to UK journalists, sources (including whistleblowers), academics and researchers who work for or collaborate with entities

[82] UK Cabinet Office, "Government Security Classifications Policy", available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1166145/Government_Security_Classifications_Policy_June_2023.pdf (June 2023) (last accessed 30 November 2023).

[83] UK Cabinet Office, "Guidance 1.1: Working at OFFICIAL", available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1166148/Guidance_1.1__Working_at_OFFICIAL.pdf (17 July 2023) 1 (last accessed 30 November 2023).

[84] Ibid., at 4–11.

(such as media organisations, public universities or research institutions) that are owned, directed or controlled by a foreign government. This is because the National Security Act provides that the requirement that conduct is "carried out for or on behalf of a foreign power" can be "satisfied by a direct *or indirect* relationship between the conduct … and the foreign power".[85] As a result, it could be possible to establish an indirect relationship between the conduct of some journalists, sources or academics and a foreign government through media organisation or public university, for example. There are countless entities that could fall within the scope of these provisions, including those owned, directed or controlled by allies. Those who work for or collaborate with such entities (or their employees) are therefore put at risk of satisfying the foreign power condition, even if those people are engaging in legitimate activities. This could include, for example, collaborating with academics from a US university or working for a New Zealand-owned media organisation.

For the foreign power condition to be met, the person must still "know[], or having regard to other matters known to them ought reasonably to know" that the conduct or course of conduct is for or on behalf of a foreign power.[86] However, it may not be difficult to prove this fault element in the context of the present example, especially as the "ought reasonably to know" standard has been included as an alternative to knowledge. For example, it could be argued that an academic ought reasonably to have known that the foreign university they were collaborating with was controlled by government, or that a journalist ought reasonably to have known that they were working for a media organisation that was owned by a foreign government, given the foreign nature of such interactions.

While the foreign power condition has the potential to be met in situations other than genuine espionage, the remaining elements of Protected Information Espionage or Trade Secrets Espionage would need to be satisfied for the person's conduct to constitute a crime. This is unlikely to occur in the context of Trade Secrets Espionage given the requirement of knowledge of unauthorised conduct. Persons (including academics and researchers) involved in the genuine handling of trade secrets are usually aware of confidentiality obligations under their employment contract; so, it is likely to be difficult to argue that they did not know that their conduct was unauthorised.

However, there are certain situations beyond genuine foreign espionage in which the remaining elements of Protected Information Espionage have the potential to be met. In such situations, any preparatory conduct (such as preliminary research, talking to people or drafting notes) could be

[85] National Security Act 2023, s. 31(3), emphasis added.
[86] Ibid., s. 31(1).

captured by the preparatory offence too. For example, UK journalists might obtain, retain or disclose information on UK military operations, intelligence agencies' policies or diplomatic relations in the course of public interest reporting. Although it might be important for such information to be made public, it may be possible to argue that the journalist's conduct was for a purpose (that is, to publish public interest stories) that they ought reasonably to have known is prejudicial to the safety or interests of the UK. It might even be possible to argue that the journalist had knowledge of this. A whistleblower or source who provides such infortmation to journalists may also commit an offence.

Given the breadth of "protected information" (applying to information that is restricted in *any* way and that need not necessarily be labelled as such), certain UK academics and researchers might also be capable of satisfying the elements of Protected Information Espionage. It could be argued that their conduct is for a purpose (to publish research) that they ought reasonably to know is prejudicial to the safety or interests of the UK. This fault element could also apply to others too, such as people who knowingly pass on "protected information" without asking the recipient about where that information might end up.

Although there have been no convictions or charges under the 2023 offences to date (so, any consideration of the scope of the offences remains hypothetical), it is possible that the new laws will be used against those involved in legitimate activities because the previous laws were used for such a purpose (along with, of course, prosecuting genuine spies). For example, in *Chandler*, several protestors who attempted to block military aircraft from taking off at a military airfield (campaigning for nuclear disarmament by non-violent means) were convicted of conspiracy and incitement to engage in Espionage by Trespass and were sentenced to 12 to 18 months' imprisonment. This case serves as a warning of the dangers of over-broad laws and the need for adequate protections for those involved in legitimate activities.

IV. Australia's Espionage Laws

Australia's "first-generation" espionage offences (which replicated those in the Official Secrets Act 1911) were introduced in 1914 in response to WWI.[87] Only one recorded case exists in which a person was prosecuted under these offences. In *R. v Lappas*,[88] the defendant, a Defence Intelligence Organisation employee, was convicted of Espionage by Information Gathering and sentenced to two years' imprisonment. Lappas had passed documents (which he annotated), revealing sources of

[87] Crimes Act 1914 (Cth), s. 78, repealed by Criminal Code Amendment (Espionage and Related Matters) Act 2002 (Cth), sched. 1, items 1, 5.
[88] [2003] ACTCA 21, (2003) 152 A.C.T.R. 7.

ongoing intelligence, to a third party, who was then to sell it to a foreign power. The attempted sales were, however, unsuccessful.

By the twenty-first century, the first-generation offences were perceived to be outdated and unreflective of the "modern intelligence environment".[89] As such, they were completely replaced in 2002 – when Australia introduced unprecedented counter-terrorism laws[90] – with the "second-generation" offences.[91] These offences criminalised a broader scope of conduct than the first-generation offences, yet they prescribed much harsher penalties. Despite this, no cases were recorded detailing prosecutions under the second-generation offences, nor were convictions secured in unreported cases[92] – perhaps partly because of ASIO's focus on counter-terrorism in the years following their introduction.

A. The 2018 Offences

Because there had been no convictions and – it was claimed – the second-generation offences had failed to "evolve[] … with the modern threat environment"[93] (and therefore Australia's "agencies lacked the legislative tools they needed to act"[94]), the 2018 reforms were introduced. These reforms consist of five underlying offences, two "espionage-related" offences and three defences. The espionage-related offences (the "Solicitation Offence"[95] and the "Preparatory Offence"[96]) prescribe maximum penalties of 15 years' imprisonment, while the more serious underlying offences prescribe maximum penalties of 20 years', 25 years' and life imprisonment. Although there are only five underlying offences, some of these have alternative fault elements (either intention or recklessness as to certain national security consequences), essentially creating nine different underlying offences. Many of these offences share common physical and fault elements. The underlying offences include: the "Core Espionage Offence";[97] "Communication Espionage";[98]

[89] Revised Explanatory Memorandum, Criminal Code Amendment (Espionage and Related Matters) Bill 2002, 5–6.
[90] Williams, "Decade of Australian Anti-Terror Laws".
[91] Criminal Code, s. 91.1, repealed by the National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018 (Cth), sched. 1, item 17. For discussion of these offences, see Kendall, "Australia's New Espionage Laws", 135–41.
[92] In 2017, then Prime Minister Malcolm Turnbull emphasised that Australia's second-generation espionage laws were "so unwieldy that they ha[d] not supported a single conviction in decades": Commonwealth, *Parliamentary Debates*, House of Representatives, 7 December 2017, 13148.
[93] Revised Explanatory Memorandum, National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (Cth), at [16].
[94] Commonwealth, *Parliamentary Debates*, House of Representatives, 7 December 2017, 13145.
[95] Criminal Code, s. 91.11.
[96] Ibid., s. 91.12.
[97] Ibid., s. 91.1.
[98] Ibid., s. 91.2.

"Classified Information Espionage";[99] "Espionage on Behalf of a Foreign Principal";[100] and "Trade Secrets Espionage".[101]

The Core Espionage Offence criminalises dealing with security classified[102] or national security information that is or will be communicated to a foreign principal. It has two different fault elements – the person intended either to "prejudice Australia's national security" or to "advantage the national security of a foreign country",[103] or they were reckless as to this prejudice or advantage.[104] Communication Espionage also has two alternative fault elements. It is an offence for a person to deal with information that is or will be communicated to a foreign principal where they either intended to "prejudice Australia's national security",[105] or were reckless as to this prejudice.[106]

Espionage on Behalf of a Foreign Principal criminalises dealing with information "on behalf of, or in collaboration with", or where the dealing is "directed, funded or supervised by", a foreign principal, where the person is reckless as to whether this involves the commission of an espionage offence.[107] In addition to those elements, the offence may also be proved where the person intended to "prejudice Australia's national security" or "advantage the national security of a foreign country",[108] or they were reckless as to this prejudice or advantage.[109] The outcome is, essentially, three different offences: Espionage on Behalf of a Foreign Principal (intention), (recklessness) or (no fault element).

Classified Information Espionage and Trade Secrets Espionage have no fault elements in relation to prejudice or advantage to national security, meaning that a person will have committed these crimes if they engage in the requisite physical conduct, regardless of whether they turned their mind to the national security consequences. Classified Information Espionage makes it an offence to deal with security classified information that is or will be communicated to a foreign principal where this is done with "the primary purpose of communicating" it to a foreign principal.[110] Where a person dishonestly obtains or discloses trade secrets on behalf of or in collaboration with, or where the dealing is "directed, funded or supervised by", a foreign principal, Trade Secrets Espionage will have been committed.[111]

[99] Ibid., s. 91.3.
[100] Ibid., s. 91.8.
[101] Ibid., s. 92A.1. For a table summarising these offences and their penalties, see Kendall, "Australia's New Espionage Laws", 143.
[102] Information with a formal classification of secret or top-secret: Criminal Code, s. 90.5(1).
[103] Ibid., s. 91.1(1)(c).
[104] Ibid., s. 91.1(2).
[105] Ibid., s. 91.2(1)(b).
[106] Ibid., s. 91.2(2).
[107] Ibid., s. 91.8(3).
[108] Ibid., s. 91.8(1)(b).
[109] Ibid., s. 91.8(2)(b).
[110] Ibid., s. 91.3(1)(aa).
[111] Ibid., s. 92A.1(1).

Australia's espionage framework includes four aggravating circumstances that apply to four of the underlying offences and operate to increase the maximum penalty available for those offences.[112] This essentially creates 16 aggravated offences and a highly complex scheme of 27 separate espionage offences.[113]

Three defences may apply to a charge of espionage under Australian law. First, it is a defence for a person to deal with the information according to a Commonwealth law or agreement, or in a person's capacity as a public official (the "Lawful Dealing" defence).[114] The first defence applies to all offences except Trade Secrets Espionage. The second defence ("Authorised Prior Publication"), which applies to all offences except Trade Secrets Espionage and the espionage-related offences, arises where the information was already "communicated … to the public with the authority of the Commonwealth".[115] The final defence ("Unauthorised Prior Publication") arises where: the information was already communicated to the public; the person was not involved in this prior publication nor was the information obtained as a result of being a Commonwealth officer; and, at the time of dealing with the information, the person had reasonable grounds for believing that doing so would not prejudice Australia's national security, "having regard to the nature, extent and place of the prior publication".[116] This defence applies only to the Espionage on Behalf of a Foreign Principal offences but also to the Core Espionage Offence (where the prosecution relies on intention or recklessness as to advantage to the national security of a foreign country).

All of Australia's espionage offences (with the exception of Trade Secrets Espionage) apply to conduct and results of conduct that occur both within and outside of Australia.[117] Trade Secrets Espionage only applies to conduct within Australia or, if the conduct occurred outside Australia, where: (1) the result of the conduct occurred in Australia, or (2) the person was an Australian citizen or resident at the time that the conduct occurred.[118]

B. Key Terms and Elements

Many of Australia's underlying espionage offences share key terms and elements. At their core, the offences criminalise *dealings* with certain *information or articles* on behalf of, or to communicate to, a *foreign principal*. Some of these offences also require that the person intends the

[112] Ibid., s. 91.6. Aggravating circumstances apply to Core Espionage (recklessness), Communication Espionage (intention and recklessness) and Classified Information Espionage.
[113] The scheme consists of nine underlying offences, two espionage-related offences and 16 aggravated offences.
[114] Criminal Code, ss. 91.4(1), 91.9(1), 91.13.
[115] Ibid., ss. 91.4(2), 91.9(2).
[116] Ibid., s. 91.4(3).
[117] Ibid., ss. 91.7, 91.10, 91.14, 15.4.
[118] Ibid., ss. 92A.2, 15.2.

conduct to prejudice Australia's *national security* or to give advantage to the national security of a foreign country, or is reckless to such prejudicing or giving advantage. Not only have these key terms been defined with incredible breadth, but some terms are also uncertain in their application.

"Deal" has been defined to cover receiving, obtaining, collecting, possessing, making a record, copying, altering, concealing, communicating, publishing or making available.[119] "Make available" has been defined to include placing the information or article somewhere to be accessed by another, giving it to an intermediary to give to the recipient, and describing how to access it or methods that may facilitate access to it (for example, by setting out "the name of a website, an IP address, a URL, a password, or the name of a newsgroup").[120] This means that dealing with information encompasses providing a password to someone, collecting information, or communicating it to another person, as well as mere passive receipt, leaving the information in a place that may be accessed by another person, or passing on the name of a newsgroup that may be able to access the information.

"Information" means "information of any kind, whether true or false and whether in a material form or not, and includes an opinion, and a report of a conversation", with "articles" meaning "any thing, substance or material".[121] Dealing with such information or articles encompasses "dealing with all or part of" it, or even the "substance, effect or description" of it.[122] While these definitions are broad enough to include documentary information, information held in electronic form and physical products of research (such as samples and prototypes), they also include false information and mere opinions. For simplicity, this article will use "information" to refer to "information or articles".

At the core of espionage is that the dealing has something to do with a "foreign principal". Foreign principals are foreign governments or their authorities, foreign political organisations, public international organisations, terrorist organisations, foreign public enterprises and entities "owned, directed or controlled by" any of these foreign principals.[123] "Foreign public enterprise" has been defined to mean a company, body or association that enjoys special legal rights or benefits under foreign law where: (1) the foreign government "holds more than 50% of the issued share capital" of, or voting power in, the company, or can "appoint more than 50% of the … board of directors"; (2) the directors of the company, body or association are accustomed to act under the directions of the foreign government; or (3) the foreign

[119] Ibid., s. 90.1(1).
[120] Ibid.
[121] Ibid.
[122] Ibid., s. 90.1(2).
[123] Ibid., ss. 90.2, 90.3.

government is "in a position to exercise control over the company", body or association.[124] Foreign public enterprises are therefore essentially entities that are owned or controlled by a foreign government.

"National security" is relevant both to the fault element of some of the offences and, for the Core Espionage Offence, to the type of information that is dealt with. Unlike the UK, which has eschewed legislative definitions of "security" and "national security" on separation of powers grounds,[125] that term has been defined in the Criminal Code Act 1995 (Cth). This is typical of Australian law, where security is traditionally legislatively defined.[126] In the espionage context, national security encompasses traditional defence matters, including: defence of the country; protection of its borders from serious threats; and protection of the country and its people from espionage, sabotage, terrorism, political violence, foreign interference and obstruction of the defence force.[127] However, it also extends beyond these matters to "the carrying out of the country's responsibilities" to other countries and "the country's political, military or economic relations with another country".[128] The breadth of this definition means that "national security" controversially includes a country's economic or international relations. In *Thomas v Mowbray*, Gummow and Crennan JJ. queried whether in certain provisions of the National Security Information (Criminal and Civil Proceedings) Act 2004 (Cth) – which use a similar definition of "national security"[129] – "the Parliament has sought to over-reach the bounds of the understanding of 'national security'".[130]

All offences – except Classified Information and Trade Secrets Espionage – require one of several fault elements to be proved. These include that the person intended to: (1) prejudice Australia's national security; or (2) advantage the national security of a foreign country. Alternatively, the person may only have been reckless as to either. "Intention" has been defined as the person: meaning to engage in the conduct or bring about the result; believing a circumstance "exists or will exist"; or being aware that a result "will occur in the ordinary course of events".[131] By contrast, "recklessness" criminalises a much lower level of culpability – all that must be shown is that the person was "aware of a substantial risk that the circumstance" or result would occur and, "having regard to the circumstances known to him or her, it [was] unjustifiable to take the risk".[132]

[124] Ibid., s. 70.1.
[125] *Home Secretary v Rehman* [2001] UKHL 47, at [50] (Lord Hoffmann).
[126] E.g. Australian Security Intelligence Organisation Act 1979 (Cth), s. 4; Criminal Code, s. 90.4(1); National Security Information (Civil and Criminal Proceedings) Act 2004 (Cth) (NSI Act), s. 8.
[127] Criminal Code, s. 90.4.
[128] Ibid., ss. 90.4(1)(d)–(e).
[129] See NSI Act, ss. 8, 9, 10.
[130] *Thomas v Mowbray* [2007] HCA 33, (2007) 233 C.L.R. 307, at [124].
[131] Criminal Code, s. 5.2.
[132] Ibid., ss. 5.4(1)–(2).

"Prejudice" has been defined only so that "embarrassment alone is not sufficient to prejudice Australia's national security".[133] Prejudice to Australia's national security could therefore encompass anything from harming Australia's security interests to making Australia (or its officials) look bad or corrupt. "Advantage" has also not been comprehensively defined – the Criminal Code only specifies that "conduct will not advantage the national security of a foreign country if" it would "advantage Australia's national security to an equivalent extent".[134] However, this still means that conduct may be criminalised where it would benefit another country, including Australia's allies, but have a neutral effect on Australia. Conduct advantaging another country may also be criminalised where the advantage to Australia may not rise to the level of the advantage to another country.

C. Espionage-Related Offences

As outlined above, Australia has two espionage-related offences. The Solicitation Offence criminalises intentionally "soliciting or procuring, or making it easier to solicit or procure", a person to engage in espionage, where this is done on behalf of a foreign principal.[135] This offence targets the conduct of recruiters of spies, not the spies themselves. It is not necessary that the recruiter have in mind a particular act of espionage for an espionage offence to be committed by the targeted person, or for it even to be possible to commit the espionage offence.[136]

The Preparatory Offence makes it a crime to engage in conduct "with the intention of preparing for, or planning, an [espionage] offence".[137] It can also arise where an espionage offence is never committed, or whether or not the person has in mind a specific offence.[138] This offence criminalises the earliest stage of a crime, even if the conduct may ultimately have an innocent explanation, provided that it could be shown from surrounding circumstances that the person means later to engage in espionage.

Although these offences are inchoate offences (or pre-crimes), they still attract general inchoate liability, with the exception of attempt.[139] Inchoate provisions of the Criminal Code include: attempt;[140] aiding, abetting, counselling or procuring;[141] joint commission;[142] commission by proxy;[143]

[133] Ibid., s. 90.1(1), emphasis removed.
[134] Ibid., emphasis removed.
[135] Ibid., s. 91.11(1).
[136] Ibid., s. 91.11(3).
[137] Ibid., s. 91.12(1).
[138] Ibid., s. 91.12(3).
[139] Ibid., ss. 91.11(4), 91.12(2).
[140] Ibid., s. 11.1.
[141] Ibid., s. 11.2.
[142] Ibid., s. 11.2A.
[143] Ibid., s. 11.3.

https://doi.org/10.1017/S0008197323000466 Published online by Cambridge University Press

incitement;[144] and conspiracy.[145] This creates somewhat confusing and broad pre-pre-crimes, such as procuring someone to solicit someone else to commit espionage, or conspiracy to prepare for espionage. This last-mentioned offence would criminalise conduct far before the commission of any substantive offence (such as merely talking to someone else about doing something that may later lead to espionage) and therefore has the capacity to capture a wider range of conduct. It greatly expands the scope of Australia's espionage laws.

D. Application of Australia's Espionage Laws

Because there have been no recorded cases involving the 2018 espionage offences, the application of Australia's espionage laws can best be understood by considering real-world scenarios in which they could arise. The Core Espionage Offence, for example, would criminalise the theft of Australian classified documents via cyber hacking by a foreign intelligence agent located overseas. Such conduct could also be prosecuted under Classified Information Espionage. The Core Espionage Offence could equally criminalise the publication of a story by a journalist that details allegedly corrupt or illegal conduct by the Australian military, such as Oakes's and Clarke's "Afghan Files". Publication to the world at large would certainly qualify as communication to a foreign principal, while the nature of the story may amount to recklessness as to prejudice to Australia's national security.[146]

Where a whistleblower communicates information to a journalist that may show Australia in a bad light, such as Witness K's revelations that ASIS bugged the East Timorese Cabinet or Smethurst's exposure of the proposed expansion of the ASD's domestic surveillance powers, Communication Espionage may have been committed. It is the job of journalists to publish information to the public; so, communication of information to journalists may result in communication to a foreign principal and also establish an intention or recklessness as to prejudice to Australia's national security on the part of the whistleblower. Mere passive receipt of this information by the journalist who then takes some preliminary investigative steps could amount to Communication Espionage.

Espionage on Behalf of a Foreign Principal could make it an offence for an Australian academic working for a public university overseas to conduct research into Australia's military capabilities or economic relations.[147]

[144] Ibid., s. 11.4.
[145] Ibid., s. 11.5.
[146] For in-depth discussion of how each of Australia's espionage offences could apply to journalists and sources, see Ananian-Welsh, Kendall and Murray, "Risk and Uncertainty"; Ananian-Welsh and Kendall, "Crimes of Communication".
[147] For in-depth discussion of how each of Australia's espionage laws could apply in the context of academic teaching and research, see Kendall, "Erosion of Academic Freedom".

However, it would also, unsurprisingly, capture situations where a foreign agent obtains sensitive information in relation to Australia. Where the information relates to trade secrets, obtaining it would be criminalised under Trade Secrets Espionage. Trade Secrets Espionage could also arise, however, where a foreign researcher collaborating with Australian researchers communicates commercially valuable information, generated as a result of the collaboration, to foreign state-owned corporations not involved in the research.

The Solicitation Offence would capture a foreign agent who tries to bribe or persuade an Australian government employee to engage in espionage. However, it could also criminalise the conduct of an academic working for a foreign public university who seeks to collaborate with an Australian researcher working on a project involving intelligence policies, or an Australian journalist working for a foreign state-controlled media organisation who enquires about whether a source has information related to Australia's security or diplomatic relations. If the journalist talks to other employees about obtaining this kind of information from a source, conspiracy to solicit espionage could have been committed.

The breadth of the Preparatory Offence means that it captures the conduct of foreign agents who take steps to engage in espionage. However, it could equally apply to Australian journalists, sources, academics and researchers by making it an offence, for example: to make a list of potential collaborators; to purchase a USB that may be used to collect and store classified documents; or to investigate which organisations may have access to certain sensitive information. The pre-pre-crime of conspiracy to prepare for espionage could similarly criminalise a wide range of behaviour, from asking a member of the defence force about the security systems used to protect military data to two academics' discussing a potential research project on Australia's international relations.

V. Effectiveness

This article's previous parts examined espionage laws in the UK and Australia and briefly considered how they could be applied in practice. Parts V and VI critically compare the two nations' espionage laws in terms of their effectiveness and appropriateness.

This article uses effectiveness to refer to the capability of laws to achieve their intended aim. In the context of espionage laws, the objective aim is to address modern espionage. As described in Part II, modern espionage can be conducted by any foreign country and typically involves using technology and the internet (cyberespionage) to collect, store and communicate valuable information. Laws that fail to capture such conduct are ineffective and redundant in today's security climate.

Whether espionage laws are capable of addressing modern espionage requires consideration of whether: the language of the offences reflects the modern intelligence environment; the offences are capable of criminalising the conduct of anyone who engages in espionage, regardless of where they are located in the world; and the offences themselves target different aspects of espionage (for example, the conduct of spies as well as of recruiters).

A. Language Reflecting the Modern Intelligence Environment

Unlike previous offences, the UK's new 2023 espionage offences and Australia's new 2018 espionage offences were drafted in modern language that reflects today's intelligence environment. For example, instead of referring to "enemies", the offences refer to "foreign power" (UK) or "foreign principal" (Australia). Both of these terms have been defined in a way that recognises that espionage is now conducted by a variety of actors, from foreign governments (even allies) and political parties to corporations, organisations and other entities that are owned or controlled by foreign governments.

Although these modern terms improve the potential effectiveness of the espionage laws, unlike Australia's definition of foreign principal, "foreign power" does not include terrorist organisations or other non-state actors (who are increasingly engaging in espionage activities). The inclusion of these actors in the definition of foreign power was something that the Law Commission specifically recommended.[148] Furthermore, in contrast to "foreign principal", "foreign power" includes only *governing* political parties. This is a significant limitation of the UK's laws, given that espionage can be (and often is) undertaken by non-governing political parties.

Despite these limitations, UK and Australian espionage offences both use modern terms to describe the form of information protected under the laws. Instead of using outdated, wartime terms, such as "sketch, plan, model, note, and secret official pass word and code word", the UK's 2023 offences refer to "any information, document or other article", while Australia's 2018 offences refer to "information and articles". Although the National Security Act 2023 has not provided much guidance as to what constitutes information, documents or articles, these terms are broad enough to include many of the forms of information targeted by modern espionage (including electronically stored data and information). It is less clear, however, whether the terms extend to other things that can be targeted by espionage, such as samples and prototypes.

The definitions of information and articles under Australia's Criminal Code are similar in scope to the terms used in the UK, in that they have

[148] Law Commission, *Protection of Official Data*, 30.

the capacity to apply to the forms of information targeted by modern (cyber) espionage. However, unlike the UK's, Australia's definition of "article" clearly indicates that it includes "any thing, substance or material".[149] Despite this, the scope of information and articles goes beyond that of the UK, unnecessarily extending to opinions and untrue information. Leaving "information and articles" undefined, though clarifying that the terms do in fact include "things", is perhaps a better approach that still ensures the laws will be effective.

B. Extraterritoriality

An advantage of the espionage frameworks in both the UK and Australia, and one of the reasons why the new laws are capable of being effective, is the territorial ambit of the offences. The espionage offences in both countries (except for Trade Secrets Espionage) apply to conduct committed by anyone anywhere in the world. The Trade Secrets Espionage offences have a slightly narrower territorial ambit than the other espionage offences, but they still have the capacity to apply beyond the borders of the UK and Australia, so long as there is some connection to those countries. For example, in the UK, the trade secret must have been in the possession or under the control of a UK person, while in Australia, the person committing the offence must have been an Australian citizen or resident. The new laws therefore have the capacity to capture espionage conducted remotely from outside the UK and Australia (as occurs through cyberespionage).

However, extraterritorial application of espionage laws does not necessarily result in someone who commits espionage abroad being prosecuted. This is because the person must be extradited to the UK or Australia (as the case may be) to face prosecution. Extradition is a complex process that requires international cooperation, with extradition requests being made through diplomatic channels. If an extradition request is made to a country that has an extradition treaty with the UK or Australia, then there are usually obligations on that country to consider the request. However, if no extradition treaty exists (or the treaty is not yet in force), it is up to the foreign country to decide whether to agree to the request and surrender the person. As a result, it may be difficult to extradite an alleged offender to the UK or Australia to face prosecution for espionage.[150] There are numerous examples of crimes being committed in the UK by known foreign agents, but these

[149] Criminal Code, s. 90(1).

[150] See e.g. the issues that have arisen with attempts to extradite Julian Assange to the US to face prosecution for espionage in relation to his role in WikiLeaks: E. Peltier and M. Specia, "U.K. Judge Blocks Assange's Extradition to U.S., Citing Mental Health", *The New York Times*, available at https://www.nytimes.com/2021/01/04/world/europe/assange-extradition-denied.html (last accessed 1 November 2023). For discussion of the difficulties that arise with extraterritorial application of US economic

https://doi.org/10.1017/S0008197323000466 Published online by Cambridge University Press

agents face no prospect of being extradited for prosecution – for example, Russia has refused the extradition of the agents responsible for the Litvinenko and Salisbury poisonings.[151]

While there may be difficulties extraditing a person to the UK or Australia to face charges of espionage, there are at least two benefits of extraterritorial criminal laws. First, such laws play an important role in furthering unilateral foreign policy objectives and communicating to other nations the kind of conduct that the country does not tolerate.[152] Second, laws that do not even provide for extraterritorial application where a hallmark of the criminal conduct is that it is typically engaged in extraterritorially *a priori* cannot be effective. Such application is necessary to ensure that the laws have the potential to allow for the prosecution of someone who committed espionage abroad – for example, if the person ever enters the UK or Australia (or another country with which the UK or Australia has an extradition treaty). Broad extraterritoriality may ultimately result in a person's being extradited to a country in which the conduct did not occur and the person is not a citizen or resident.[153] Espionage, however, is inherently a harm against the State, and such harm should be the determining factor in deciding whether espionage laws apply to a particular person – not that person's citizenship status or location in the world.

C. Offences Targeting Different Aspects of Espionage

A further benefit of the espionage frameworks in both the UK and Australia is that they contain different offences which cover a variety of conduct related to espionage. This coverage enhances the potential effectiveness of the offences in the modern espionage context. For example, both countries have an offence for Trade Secrets Espionage. This type of offence targets a very specific type of information that is distinct from traditional national security information, yet that specific type is targeted by today's espionage. It is targeted through the theft of trade secrets from companies to assist state-sponsored foreign entities in skipping or accelerating the "research and development" phase of product development, which ultimately benefits the country's economy.[154]

espionage laws, see B.I. Rowe, "Transnational State-Sponsored Cyber Economic Espionage: A Legal Quagmire" (2020) 33 Security Journal 63.

[151] R. Owen, *The Litvinenko Inquiry: Report into the Death of Alexander Litvinenko*, HC 695 (London 2016); H. Siddique, "Third Russian National Charged over Salisbury Poisonings", *The Guardian*, available at https://www.theguardian.com/uk-news/2021/sep/21/third-russian-national-charged-over-salisbury-poisonings (last accessed 1 November 2023).

[152] E.g. D. Ireland-Piper, "Extraterritorial Criminal Jurisdiction: Does the Long Arm of the Law Undermine the Rule of Law?" (2012) 13 Melbourne Journal of International Law 122.

[153] E.g. the US is seeking to extradite Assange, an Australian citizen, from the UK, yet Assange was not in the US when the leaks occurred.

[154] M. Reid, "A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing with This Global Threat?" (2016) 70 University of Miami Law Review 757, 760–61.

A specific offence for this type of conduct is argued to be necessary because of the unique nature of this type of espionage,[155] and its inclusion in UK and Australian law makes their espionage frameworks particularly capable of addressing the modern espionage threat.

Another aspect of the espionage frameworks in both countries that is especially advantageous is the inclusion of specific inchoate espionage – in Australia, the espionage-related offences (the Solicitation and Preparatory Offences), and in the UK, the preparatory offence. These offences are key to an effective legal response to the modern espionage threat.[156]

The Solicitation Offence (which could be created in the UK by pairing the inchoate offence of solicitation with any of the underlying espionage offences) ensures that the law is capable of holding those who recruit (or attempt to recruit) others to engage in espionage criminally responsible. This offence does not criminalise the conduct of the target, who may not have committed an offence or who may have been led to commit espionage through blackmail or bribes.[157] Knowing that the law criminalises soliciting someone to commit espionage, not just the conduct of spies, may also be an effective deterrent for recruiters.

The preparatory offences criminalise the very early stages of committing an espionage offence, potentially before a specific offence is committed or even identified. They may also operate to deter any sort of conduct related to spying and give law enforcement agencies the power to investigate and charge someone before they commit espionage. The inchoate espionage offences therefore have the potential to be considerably effective at addressing modern espionage, both through deterrence and the criminalisation of a wider scope of conduct.

D. Summary

The espionage laws in the UK and Australia are capable of effectively dealing with modern espionage. This is because the laws in each jurisdiction use modern language that reflects the espionage that is engaged in today (although there are some limitations with how certain key terms have been defined in the UK). They also have wide extraterritorial application and include offences targeting different aspects of espionage (such as espionage of trade secrets, the solicitation of espionage and preparations for espionage). The next part considers the appropriateness of espionage laws in the UK and Australia, highlighting the importance of balancing effectiveness with appropriateness.

[155] Ibid.
[156] Kendall, "Australia's New Espionage Laws", 157.
[157] Ibid., 152–53.

https://doi.org/10.1017/S0008197323000466 Published online by Cambridge University Press

VI. Appropriateness

When assessing laws, effectiveness cannot be the only consideration – laws must also be appropriate. Without this second stage of analysis, there is a risk that laws that are capable of being highly effective are also far too wide-reaching and undermine fundamental rule of law values and legal principles, such as clarity in the law. I use appropriateness in this article to refer to: (1) the clarity of the laws; and (2) whether the laws are appropriate in scope.

A. Clarity

Appropriateness requires laws to be clear to avoid uncertainty or ambiguity. Some laws may be intentionally drafted in an unclear manner – deliberately to widen the scope of conduct captured or to allow for changes over time in how certain criminal conduct is performed.[158] While these rationales may be legitimate, they go to the *effectiveness* of criminal laws, not their appropriateness. Laws must be clear not only to ensure that citizens understand their obligations under the law and know whether they are committing an offence, but also so that jurors can effectively apply the law in cases that come before the courts. If laws do not do this, then they are not appropriate.

The complexity of Australia's espionage framework and some aspects of the UK's espionage framework, as well as the uncertainty of key terms in both jurisdictions, make their espionage laws unclear in certain ways and therefore not as appropriate as they could be.

1. Complexity of espionage frameworks

Australia's 2018 reforms created a highly complex scheme of 27 espionage offences with different penalties for each offence and various defences that apply only to some offences. Many of the offences overlap, so that certain conduct may be criminalised under a number of different offences. For example, espionage of classified information could fall under the Core Espionage Offence, Classified Information Espionage or the Preparatory Offence. To its advantage, the UK has a scheme of only three offences, each targeting a distinct type of conduct. This distinct targeting makes its espionage laws far simpler and clearer than Australia's espionage laws.

Despite the simplicity of the UK's framework, it does include a preparatory offence. Similarly, Australia's espionage framework includes the espionage-related offences of solicitation and preparation. As

[158] In the counter-terrorism context, see B. Golder and G. Williams, "What Is 'Terrorism'? Problems of Legal Definition" (2004) 27 University of New South Wales Law Journal 270, 293; N. McGarrity, "'Testing' Our Counter-Terrorism Laws: The Prosecution of Individuals for Terrorism Offences in Australia" (2010) 34 Criminal Law Journal 92, 114–15.

discussed above, it is possible for these inchoate espionage offences themselves to attract general inchoate liability found elsewhere in the law. This creates complicated espionage schemes in the UK and Australia, where it can be an offence to procure someone to solicit someone else to commit espionage, or for two people to conspire to prepare for espionage. The espionage frameworks in the UK and Australia could be clearer if their inchoate espionage offences did not themselves attract general inchoate liability. Greater clarity could be achieved by specifically indicating in espionage legislation that general inchoate provisions found elsewhere in the law do not apply (as with the non-application of attempt to Australia's espionage-related offences).

2. Uncertainty of key terms

While Australia's espionage legislation has defined most of its key terms, many of these definitions are uncertain in scope. "Foreign principal", for example, has been defined to include "foreign government principals". "Foreign government principals" includes "foreign public enterprises" which is itself defined in a lengthy and complex manner, but could include such entities as foreign state-controlled companies or associations. However, such entities could also fall easily within the "entities owned, directed or controlled by a foreign principal" aspect of the definition of foreign principal.

In addition to the uncertain and complex definition of foreign principal, "prejudice" and "advantage" have not been comprehensively defined. Furthermore, "national security" has been defined to mean defence matters but also, controversially (and beyond traditional notions of "security"), political or economic relations with another country. What does it mean to prejudice Australia's national security, conceived as Australia's economic relations with another country? Is information about Australia's international relations "national security information"? Exactly how far does "national security" reach? These and similar questions pose problems not just for people who deal with this information in their professional capacity, such as government employees or investigative journalists, but also for jurors attempting to apply these laws. The uncertain reach of "national security" is further exacerbated by the breadth of "information", which includes opinions and untrue information.

Although many of the key terms used in Australia's legislation are uncertain, some of the key terms used in the UK's National Security Act are also not as clear as they could be. For example, it is unclear whether "information, documents and other articles" extends to things such as scientific samples or prototypes. Additionally, although "foreign power" does not explicitly include entities owned, directed or controlled by a foreign power (as is included in Australia's definition of foreign

principal), the definition of "foreign power condition" stipulates that whether a person's conduct was carried out for or on behalf of a foreign power can be established by showing a direct or indirect relationship between the conduct and the foreign power (such as "through one or more companies"[159]). This would seem to draw entities that are owned, directed or controlled by a foreign power within the scope of "foreign power", without explicitly stating so.

Furthermore, "safety or interests of the UK" has not been defined in the National Security Act, creating uncertainty as to its meaning and scope. While a similar term used in previous offences ("safety or interests of the State") was judicially considered, that term was held to mean the fairly ambiguous "objects of State policy" (essentially, whatever the state said was in its safety or interests).

3. Summary

Several key terms in both the UK and Australia are uncertain in scope. These include, for example, "foreign principal", "national security", "prejudice" and "advantage" in Australia, and "foreign power" and "safety or interests of the UK" in the UK. Further, both frameworks are complicated by the inclusion of inchoate espionage offences which may attract general inchoate liability. Despite this, the UK's espionage framework is considerably less complex, and therefore far more appropriate, than Australia's framework as it consists of just three distinct espionage offences (compared to 27 offences in Australia).

B. Appropriate Scope

In addition to clarity, appropriateness requires consideration of whether laws are proper in scope. Again, wide-reaching offences may be *effective*, but this does not mean that they are appropriate. While governments may use broad offences to prosecute and deter innocent conduct that they deem to be distasteful (such as using espionage laws to target whistleblowers or journalists who reveal government misconduct, or protestors advocating for governmental change), this is an inappropriate use of the criminal law. Criminal offences should not capture genuinely innocent conduct or, if they do, they should provide adequate protections for innocent behaviour that may fall within the offences.

The espionage laws in the UK and Australia are not appropriate in scope because they have overly broad physical and fault elements, both frameworks include sweeping inchoate espionage offences (which are even more wide-reaching because they attract general inchoate liability),

[159] National Security Act 2023, s. 31(3).

and neither country includes adequate defences for legitimate conduct that may fall within the offences. While other safeguards may be available in both the UK and Australia to protect those engaged in legitimate conduct, these safeguards have their limitations.

1. Over-broad physical elements

Australia's espionage offences are too broad, largely because of the wide-reaching definitions of "national security", "foreign principal", "information" and "deals with". Because of how these terms have been defined, mere passive receipt of an opinion on Australia's international relations by an employee of a public international organisation or foreign state-controlled organisation (such as a foreign state-owned media organisation or public research university) could be criminalised, if the remaining elements of the offence are established.

Two of Australia's espionage laws – Communication Espionage and Espionage on Behalf of a Foreign Principal – do not limit the type of information that is dealt with. Rather, the information can be of any kind, so long as the other physical and fault elements of the offences are satisfied. This lack of limitation makes these two offences significantly wide-reaching. Australia's remaining espionage laws (the Core Espionage Offence, Classified Information Espionage and Trade Secrets Espionage) all require the information to be of a certain kind – national security, security classified or trade secrets information. This limits to some extent the reach of these offences, although as discussed above, national security information is defined with significant breadth.

Many of Australia's espionage offences are intended to be further limited by the requirement that dealing with the information does or might result in communication to a foreign principal. However, this element is broad enough to include publication (or potential publication) to the world at large – all that is necessary is that a foreign principal may receive the information in some way. Inclusion of such publication poses particular problems for whistleblowers who leak information on the internet (as Assange and Snowden did), as well as for journalists and academics, whose job it is to publish news and research to the public (which could include information amounting to national security information).[160] Indeed, Smethurst's reporting on ASD powers and Oakes's and Clarke's "Afghan Files" were both important public interest stories.

Further, communication to a foreign principal could be established where, for example: Australian journalists working for foreign state-owned media organisations talk to colleagues about stories involving Australia's national security or international relations; sources provide relevant information to

[160] Ananian-Welsh, Kendall and Murray, "Risk and Uncertainty"; Kendall, "Erosion of Academic Freedom".

https://doi.org/10.1017/S0008197323000466 Published online by Cambridge University Press

such organisations or their employees; or Australian academics collaborate with colleagues from foreign public universities on such topics.[161]

Ultimately, Australia's espionage offences have the potential to capture a range of legitimate conduct, such as conduct by certain journalists, whistleblowers, academics and researchers, especially as the fault elements are also over-broad (discussed below).

A wide-reaching physical element akin to Australia's requirement that the dealing does or might result in communication to a foreign principal is not found in the UK's offences. Rather, the foreign power condition will only be met if the conduct is instigated, directed or controlled by, or carried out on behalf of, with financial or other assistance from, in collaboration with or, with the agreement of, a foreign power. In this way, the UK's espionage laws require a stronger connection between the person's conduct and the foreign power than do Australia's offences.

Overly broad physical elements, however, are not just characteristic of Australia's espionage framework. In the UK's framework, there is, for example, the breadth and uncertainty of terms, such as "protected information" (which includes any "Official" information, even if it is not strictly sensitive or harmful) and "foreign power condition" (which could include entities owned, directed or controlled by foreign powers). Their breadth and uncertainty means that Protected Information Espionage could potentially apply to certain UK journalists, whistleblowers, academics and researchers. Specifically, it could apply to those who obtain or disclose information that might be restricted (but is not particularly sensitive), where they work for or collaborate with foreign state-controlled media organisations, universities or research institutions. Of course, to be a crime, relevant fault elements must also be established. But, as discussed below, these are also overly broad.

2. Over-broad fault elements

Some of Australia's espionage offences are supposed to be limited by proving a fault element. While "intention to prejudice Australia's national security" captures those people who genuinely engage in espionage to harm Australia, recklessness as to this prejudice significantly broadens the scope of conduct criminalised under the offences. For example, recklessness could make it a crime for a journalist to publish a public interest story based on classified information, or for an academic to publish research based on information obtained through interviews of government employees.[162] Additionally, the Core Espionage Offence and Espionage on Behalf of a Foreign Principal offences include a fault

[161] Ibid.
[162] Ibid.

element of intending to, or being reckless as to, whether the person's conduct would "advantage the national security of a foreign country". While this covers situations where a foreign country would benefit from the espionage, it is not necessary that Australia's national security actually be harmed – it could, instead, remain unaffected. Such a fault element further widens the scope of the offences.

Notwithstanding the lack of a requirement that Australia's national security actually be harmed, three offences – Classified Information Espionage, Trade Secrets Espionage and Espionage on Behalf of a Foreign Principal (with no fault element) – do not have fault elements in relation to prejudice or advantage to national security. These offences are therefore as broad as their physical elements allow and could criminalise conduct that is engaged in for an entirely innocent reason (such as exposing government wrongdoing).

The UK's espionage laws also include overly broad fault elements. Both Protected Information and Trade Secrets Espionage include the fault element of knowledge (either that the person's conduct is for a purpose that the person knows is prejudicial to the safety or interests of the UK, or the person knows that the conduct is unauthorised).[163] This fault element is appropriate in scope, capturing only those people who *know* that their conduct has a particular character or will result in a particular consequence.[164] However, both of these offences also include a more wide-reaching alternative fault element: that, having regard to other matters known to them, the person ought reasonably to know.[165] This element expands the scope of the espionage offences to people with a less culpable state of mind (such as journalists, whistleblowers and academics), applying in a similar way to the way "recklessness" does under Australian law.

3. Inchoate offences

As discussed above, both the UK and Australian espionage frameworks include inchoate espionage offences, which significantly extend the scope of conduct criminalised beyond the bounds of what is appropriate. While soliciting espionage effectively captures the conduct of recruiters of spies, it could also criminalise, for example, academics who seek national security-related information from someone working in the field or journalists who request information from sources. Australia's Solicitation Offence at least requires that the solicitation occur on behalf of a foreign principal, but this could still capture the legitimate conduct of employees of foreign state-controlled organisations (such as media organisations, universities or research institutions).

[163] The foreign power condition also includes this fault element: National Security Act 2023, s. 31(1).
[164] This fault element is equivalent to knowledge under Australian law: Criminal Code, s. 5.3.
[165] The foreign power condition also includes this fault element: National Security Act 2023, s. 31(1).

Preparing for espionage is an even more wide-reaching offence that criminalises any act done to prepare for espionage, even though such conduct may ultimately have an innocent explanation. This could include, for example, taking steps to write a public interest story or research article pertaining to Australia's national security, or purchasing a laptop that could potentially be used to commit espionage. If found guilty of this offence, a person could face up to 15 years' or life imprisonment (in Australia or the UK, respectively).

Likewise, other inchoate offences found elsewhere in the law – such as attempt, conspiracy and incitement – greatly broaden the scope of criminalised conduct, making it illegal, for example, to talk to others about engaging in conduct that could fall within the scope of an espionage offence. Like the inchoate espionage offences, these pre-crimes criminalise conduct *before* the commission of any substantive offence (and usually do not require the actual commission of a substantive offence, nor for the commission of such an offence to be possible). They thus extend the criminal law beyond its traditional bounds.

Further contributing to the over-breadth of espionage laws in the UK and Australia, their inchoate espionage offences attract general inchoate liability. Such liability creates pre-pre-crimes, for example, of procuring someone to solicit someone else to commit espionage, of conspiracy to prepare for espionage or, in the UK, of attempting to prepare for espionage.[166] Conspiracy to prepare, in particular, criminalises conduct far before the commission of any substantive offence, including two people merely having a conversation about doing something which *might* lead to espionage later. Conspiracy to prepare has routinely been used in the counter-terrorism context in Australia,[167] with people being convicted on the basis of, for example, holding meetings to discuss committing a potential terrorist act,[168] or asking a sheikh whether it is permissible under Islam to engage in a terrorist attack against the Australian army on domestic soil (to which the sheikh answered in the negative and no further action was taken by the group).[169] Those convicted of conspiracy to prepare for terrorism have been sentenced to lengthy periods of imprisonment.[170]

As in the case of the inchoate espionage offences themselves, inchoate espionage offences that attract general inchoate liability do not require a substantive offence to have been committed (or even to be possible) and distort the traditional focus of the criminal law even further. These

[166] "Attempting to prepare" is an incompatible offence in Australia: Kendall, "Australia's New Espionage Laws", 154.
[167] A. Lynch, N. McGarrity and G. Williams, *Inside Australia's Anti-Terrorism Laws and Trials* (Sydney 2015), 35–38. Criminal Code, s. 101.6(1) criminalises "[preparing] for, or planning, a terrorist act".
[168] *R. v Khalid* [2017] NSWSC 1365.
[169] *DPP (Cth) v Fattal* [2013] VSCA 276.
[170] E.g. *R. v Abbas* [2018] VSC 553 (24 years); *R. v Dirani (No. 34)* [2019] NSWSC 1005 (28 years).

pre-crimes and pre-pre-crimes significantly increase the scope of conduct that is criminalised as espionage and have the capacity to entrap people who have not engaged in genuine espionage – such as journalists, whistleblowers, academics or researchers. While such criminalisation may be the (hidden) intention of legislators, it is not an appropriate use of espionage laws.

4. Inadequate defences for legitimate conduct

Australia's espionage offences are inappropriately wide-reaching (being capable of criminalising conduct that should not be considered "espionage") and yet their breadth is not offset by adequate defences for legitimate conduct. As discussed above, Australia's espionage framework includes three defences, namely, the Lawful Dealing, Authorised Prior Publication and Unauthorised Prior Publication defences.

Lawful Dealing and Authorised Prior Publication essentially provide protections only where the information was dealt with on the Commonwealth's terms. If these defences did not exist, it is unlikely that the Commonwealth would take issue with such dealings. Nevertheless, they do provide an added layer of protection for persons legitimately dealing with information in such circumstances. For example, the first defence would protect whistleblowing made under the Public Interest Disclosure Act 2013 (Cth). However, that Act generally does not protect disclosures that may amount to espionage, especially if the information dealt with relates to "intelligence information" (which includes information relating to intelligence agencies, as well as "sensitive law enforcement information").[171]

Unauthorised Prior Publication provides greater protections than the first two defences, but it is still limited by the type of information published and the manner of initial publication. If the information relates to Australia's defence, intelligence or international relations and was initially published innocuously (such as in a blog post that is not followed by many people), republishing such information could reasonably prejudice Australia's national security, especially if it is republished in a forum that is more widely viewed (such as via a news platform or in an academic article).

Australia's three existing defences are therefore likely to be insufficient to protect most legitimate conduct which, by its nature, may attract the operation of espionage laws, such as public interest reporting, whistleblowing or academic research. Further, not all defences apply to all espionage offences. In practice, therefore, Australia's legislative defences provide inadequate protection for legitimate conduct. Although Australia's defences may not be as appropriate as they could be, the UK has failed to provide any explicit defences in the National Security Act at all.

[171] Public Interest Disclosure Act 2013 (Cth), s. 41.

5. Other safeguards for legitimate conduct

While other safeguards exist in the UK and Australia to protect legitimate conduct (such as requiring the Attorney General's consent to prosecute, and applying principles of statutory interpretation and human rights protections), these safeguards have limitations which undermine, to some extent, the appropriateness of the espionage laws in each county.

First, in each jurisdiction, proceedings for an espionage offence cannot be commenced without the Attorney General's consent, as the result of which the Attorney General has the power to decide whether or not to prosecute someone engaged in legitimate conduct.[172] However, this requirement does not ensure that all those engaged in legitimate activities (who satisfy elements of an espionage offence) are going to be protected from prosecution. While Australian law enforcement and intelligence agencies may claim not to investigate and prosecute behaviour that should be innocent,[173] there is nothing stopping a future Australian government from doing so.[174] In the UK, such conduct has already been the subject of criminal convictions.[175]

Second, certain principles of statutory interpretation can be applied to resolve ambiguities in the law, if the meaning of the espionage laws is raised as an issue before the courts. For example, in the UK, the principle against doubtful penalisation provides that "a person should not be penalised except under clear law" and that, when considering which construction to give a provision, courts should "strive to avoid adopting a construction which penalises a person where the legislator's intention to do so is doubtful".[176] Similarly, in Australia, the principle of legality can be applied to read down an uncertain provision to resolve any ambiguity in favour of the protection of fundamental common law rights, freedoms and principles.[177]

While principles such as these have the potential to resolve uncertainties in the espionage laws such that they do not apply to legitimate conduct, to reach that outcome a relevant case would have to go to court, potentially in respect of a number of different legitimate activities. This may take a long time, or may never occur. In the meantime, lack of clarity over the scope of the offences (offences which have the potential to be broad) could have a

[172] National Security Act 2023, s. 37(2); Criminal Code, s. 93.1.

[173] ASIO's Director-General has stated that "we do not investigate journalists for their journalism, academics for their research or politicians for their politics … [W]e do not investigate peaceful protests": ASIO, "Annual Threat Assessment".

[174] See further Kendall, "Erosion of Academic Freedom", 529.

[175] *Chandler v DPP* [1964] A.C. 763.

[176] D. Bailey and L. Norbury, *Bennion on Statutory Interpretation*, 7th ed. (London 2017), 715–16.

[177] E.g. D. Meagher, "On the Wane? The Principle of Legality in the High Court of Australia" (2021) 32 Public Law Review 61, 64; B. Chen, "The Principle of Legality: Issues of Rationale and Application" (2015) 41 Monash University Law Review 329, 340–42.

chilling effect on various legitimate activities, including public interest journalism and academic research and teaching.[178]

Third, in the UK, public authorities (including courts, tribunals and persons exercising public functions) must act and legislation "must be read and given effect in a way which is compatible" with rights found in the European Convention on Human Rights.[179] These requirements could be used to resolve ambiguities in the UK's espionage offences and to control prosecutorial discretion in favour of the protection of relevant Convention rights. However, Convention rights are not necessarily absolute. For example, the freedom of expression found in Article 10 (which has been held to extend to journalists, sources, whistleblowers and academics) can be subject to restrictions that are prescribed by law, pursue a legitimate aim (such as the interests of national security) and are necessary in a democratic society.[180] Additionally, this safeguard is also limited by the scope of Convention rights themselves – there may be instances of legitimate conduct that do not fall within any existing right. In Australia, there is no Federal Bill of Rights to which public action is subject.

VII. Conclusion

This article analysed the effectiveness and appropriateness of espionage laws in the UK and Australia. While the espionage laws in both countries are largely capable of effectively addressing modern espionage, this capability has come at the expense of appropriateness – specifically, aspects of the laws in both jurisdictions are complex, uncertain and overly broad, and defences and other safeguards for legitimate conduct have limitations.

The article argued that, while the effectiveness of laws is an important consideration, it must be balanced with appropriateness. If effectiveness is the only consideration, there is a risk that laws will be deliberately drafted with great breadth or lack of clarity, so that law enforcement and intelligence agencies are given the broadest powers possible to investigate and prosecute alleged "espionage". But criminal laws must not exceed their legitimate bounds and must be sufficiently clear so that laypeople can understand their obligations under the law – they must also be appropriate. By carefully considering these two principles – effectiveness and appropriateness – espionage (and other national security) laws can be created that will robustly address the growing threat, without undermining core rule of law values and legal principles.

[178] For more on the limitations of the principle of legality in the context of Australia's espionage laws, see Kendall, "Erosion of Academic Freedom", 530–32.
[179] Human Rights Act 1998, ss. 3(1), 6.
[180] European Court of Human Rights, "Guide on Article 10 of the European Convention on Human Rights: Freedom of Expression", available at https://www.echr.coe.int/documents/d/echr/guide_art_10_eng (last accessed 1 November 2023).

https://doi.org/10.1017/S0008197323000466 Published online by Cambridge University Press