The Erosion of Academic Freedom: How Australian Espionage Law Impacts Higher Education and Research

Sarah Kendall*

Abstract

In this article, I assess the impact of Australia's espionage laws on higher education and research and, consequently, on academic freedom. I find that the espionage laws have the capacity to criminalise the legitimate work of particular academics, potentially chilling research into and teaching on certain areas. The criminalisation of legitimate academic teaching and research poses risks for the academics involved (who could face up to life imprisonment) and for the state of academic freedom in Australia. Not only does this undermine the pursuit and dissemination of knowledge for the benefit of society, but it is a threat to Australia's democracy. It is crucial, therefore, that the freedom of academics to research and teach is not unduly undermined by criminal laws. As such, I conclude the article with recommendations for how Australia's espionage laws can be reformed so that genuine espionage against the higher education and research sector is criminalised while protecting academics who pursue legitimate teaching and research endeavours.

Please cite this article as:

Sarah Kendall, 'The Erosion of Academic Freedom: How Australian Espionage Law Impacts Higher Education and Research' (2022) 44(4) *Sydney Law Review* 503.

 ISSN: 1444–9528

* PhD Candidate, Sessional Academic and Senior Research Assistant, The University of Queensland School of Law, St Lucia, Queensland, Australia.
Email: s.kendall@uq.net.au; ORCID iD: https://orcid.org/0000-0002-9320-9895.
I would like to thank Associate Professor Rebecca Ananian-Welsh and the anonymous reviewers for their invaluable feedback on earlier drafts.

I Introduction

In March 2022, the Parliamentary Joint Committee on Intelligence and Security ('PJCIS') found that the higher education and research sector[1] had been (and continues to be) a target for espionage and data theft.[2] Specifically, foreign powers had been targeting the sector for research that could be commercialised or used for national gain purposes, including research on technologies with a military, energy, medical, agricultural and manufacturing application.[3] The Committee noted that, while sectors across Australia were being targeted by foreign adversaries, the higher education and research sector was a key target because of the high value it provides — in particular, '[u]niversities are at the cutting edge of sensitive research; hold large student populations from a variety of groups; and have strong access into both industry and government.'[4]

Just four years before the PJCIS released these findings in its report on the *Inquiry into National Security Risks Affecting the Australian Higher Education and Research Sector* ('PJCIS Inquiry'),[5] the Federal Government rushed a suite of new national security laws through Parliament.[6] These included new laws for espionage found in the *Criminal Code*.[7] At the time, Prime Minister Malcolm Turnbull claimed that these reforms were necessary because previous laws were 'unwieldy' and the threat of espionage had 'reache[d] unprecedented levels'.[8] Since their introduction, however, the espionage laws have been criticised by scholars for being overly broad

1 Defined as entities engaged in: 'tertiary teaching; research; the commercialisation of research with origins in the sector; grants and funding decisions in relation to the above activities; tertiary education-related representative bodies, coordination bodies or institutional groupings; and regulation of the above activities': Parliamentary Joint Committee on Intelligence and Security ('PJCIS'), Parliament of Australia, Inquiry into National Security Risks Affecting the Australian Higher Education and Research Sector (Report, March 2022) vii ('*PJCIS Report*'). In this article, I use 'research' to mean all aspects of the research process — from developing research questions, reviewing the literature, and designing the project to data collection and analysis, write-up of results, and dissemination of project findings.

2 Ibid 115, 125–6. For more on how (and why) foreign actors have been targeting research institutions and their staff, at least according to the Australian Security Intelligence Organisation ('ASIO') and the Australian Federal Police ('AFP'), see ASIO, Submission No 31 to PJCIS, *Inquiry into National Security Risks Affecting the Australian Higher Education and Research Sector* (18 December 2020) 4 [10]–[11]; AFP, Submission No 49 to PJCIS, *Inquiry into National Security Risks Affecting the Australian Higher Education and Research Sector* (January 2021) 3–4.

3 *PJCIS Report* (n 1) 125.

4 Ibid 126.

5 Ibid.

6 'National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018', *Parliament of Australia* (Web Page, 29 June 2018) <https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r6022>. See *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth).

7 *Criminal Code Act 1995* (Cth) sch 1 ('*Criminal Code*') divs 91, 92A.

8 Commonwealth, *Parliamentary Debates*, House of Representatives, 7 December 2017, 13148 (Malcolm Turnbull).

and encroaching on fundamental rights and freedoms.[9] For example, they may criminalise good faith journalism[10] or legitimate social media use.[11]

Despite the growing body of literature on the 2018 espionage (and other national security) laws,[12] scholars have yet to examine how the laws impact on the work of academics and, as such, how the laws affect academic freedom. As will be explored below, the espionage laws target dealings with information, which is at the core of what academics do. Some of these dealings may, in fact, be illegitimate — that is, undertaken for criminal purposes. This would include dealings for the purposes of espionage against the higher education and research sector, whether by academics or those from outside the academy. The vast majority of dealings by academics are, however, engaged in for legitimate research and teaching endeavours (that is, not for the purpose of criminal activity, including espionage).

If legitimate academic work is criminalised, this poses a risk not just for the academics involved (who could face up to life imprisonment), but also for the state of academic freedom in Australia. Academic freedom is fundamental to democracy.[13] It protects the freedom of academics to teach, research and disseminate the results of their research (among other things), contributing to the development of new knowledge and teaching the next generation the skills to think democratically.[14] Criminalisation of legitimate research and teaching inherently erodes academic freedom by making it illegal to pursue — and potentially punishing people for pursuing — certain intellectual inquiries.[15] Not only does this undermine the pursuit of knowledge for the benefit of society, but it poses a risk to Australia's democracy.

In this article, therefore, I assess the impact of Australia's espionage laws on higher education and research, focusing on whether (and how) the laws pose a risk to legitimate research and teaching and, consequently, to academic freedom. This is not the first time that national security laws have had an impact on academic freedom. For example, the Australian Government has historically enacted laws and promoted policies that required university staff to suppress or monitor certain types

9 See, eg, Sarah Kendall, 'Australia's New Espionage Laws: Another Case of Hyper-Legislation and Over-Criminalisation' (2019) 38(1) *University of Queensland Law Journal* 125 ('Australia's New Espionage Laws'); Rebecca Ananian-Welsh, Sarah Kendall and Richard Murray, 'Risk and Uncertainty in Public Interest Journalism: The Impact of Espionage Law on Press Freedom' (2021) 44(3) *Melbourne University Law Review* 764; Rebecca Ananian-Welsh and Sarah Kendall, 'Crimes of Communication: The Implications of Australian Espionage Law for Global Media' (2022) 27(1) *Communication Law and Policy* 3.

10 Ananian-Welsh, Kendall and Murray (n 9); Ananian-Welsh and Kendall (n 9).

11 Sarah Kendall, 'You Could Break Espionage Laws on Social Media Without Realising It', *The Conversation* (online, 14 January 2021) <https://theconversation.com/you-could-break-espionage-laws-on-social-media-without-realising-it-151665>.

12 See, eg, Kendall, 'Australia's New Espionage Laws' (n 9); Ananian-Welsh, Kendall and Murray (n 9); Ananian-Welsh and Kendall (n 9); Sarah Kendall, 'How Australia's Foreign Interference Laws Undermine Press Freedom' (2022) 47(2) *Alternative Law Journal* 124.

13 See below Part II.

14 Ibid.

15 This argument has been made in the counter-terrorism context: see Eric Barendt, *Academic Freedom and the Law: A Comparative Study* (Hart Publishing, 2010) ch 8.

of speech.[16] Whether Australia's espionage laws effectively capture genuine espionage against the higher education and research sector will not be examined, as this has been considered elsewhere.[17]

In Part II, I provide an overview of the principles of academic freedom. In Part III, I explain Australia's espionage framework and analyse how the laws impact academics who engage in legitimate research and teaching. My analysis finds that, concerningly, the espionage laws may criminalise the work of particular academics and, therefore, undermine academic freedom. In Part IV, I make recommendations for how the laws can be reformed so that genuine espionage against the higher education and research sector is criminalised, while protecting academics who pursue legitimate research and teaching endeavours.

II Academic Freedom

Academic freedom protects a university's function of independently and authoritatively advancing and disseminating knowledge.[18] It is related to, but distinct from, freedom of speech, which is a political freedom that is central to the proper functioning of democratic nations.[19] Because academic freedom protects activities related to university teaching and research (and anyone involved in those activities, including research assistants, PhD students and librarians), it applies in narrower circumstances than freedom of speech.[20] Despite this, scholars have argued that academic freedom is stronger than (and takes primacy over) freedom of speech: that is, academics should have more freedom than other university employees (and citizens generally) to discuss their work and criticise university governance because of their unique role in society.[21] Outside these areas, academics exercise their general right to freedom of speech and are subject to the same limitations as everyone else.[22]

According to scholars, there are two principal justifications for why universities — and academic freedom — are important. First, universities pursue and disseminate knowledge for the public good using independently developed research methods, and academic freedom safeguards their capacity to do so.[23] The research produced by universities benefits society immensely (take, for example, the development of new vaccines), but the advancement of knowledge requires the free inquiry and systematic testing of ideas.[24] Second, academic freedom is vital to a healthy democracy.[25] At the heart of the democratic ideal is the free flow of

16 Carolyn Evans and Adrienne Stone, *Open Minds: Academic Freedom and Freedom of Speech in Australia* (La Trobe University Press, 2021) 18–24, 66. For more on how national security laws and policies (specifically those relating to counter-terrorism) have impacted freedom of speech more generally: see Katherine Gelber, *Free Speech after 9/11* (Oxford University Press, 2016).

17 See, eg, Kendall, 'Australia's New Espionage Laws' (n 9).

18 Evans and Stone (n 16) 12, 47, 51. For more on academic freedom, see Barendt (n 15).

19 Evans and Stone (n 16) 47; Barendt (n 15) 17–22. See also *Ridd v James Cook University* (2021) 394 ALR 12, 15 [5] ('*Ridd v JCU*').

20 Evans and Stone (n 16) 56, 63–4.

21 Ibid 12–3.

22 Ibid 13, ch 4.

23 Ibid 48–53.

24 Ibid 48, 52.

25 Ibid 53–4.

information and ideas, which fundamentally rests on the pursuit of truth and knowledge.[26] Not only does academic research produce the knowledge and ideas that are necessary for the rational exchange of information, but the academy trains the next generation to critically analyse, to question and to challenge established orthodoxies — crucial skills for democratic thinking.[27] Erosion of academic freedom, therefore, not only undermines the pursuit of knowledge that benefits society, but also threatens a core value of the democratic tradition.

Despite the central importance of academic freedom to the functioning of democracies and universities, it is not referred to in Australian human rights Acts,[28] nor is it protected in the *Australian Constitution* (unlike other national constitutions, such as Japan,[29] South Africa,[30] Spain[31] and Germany[32]).[33] Australian universities do, however, have a statutory obligation under the *Higher Education Support Act 2003* (Cth) ('*HESA*') to uphold 'freedom of speech and academic freedom'.[34] Prior to 2021, this was an obligation to uphold 'free intellectual inquiry',[35] a term which was often used interchangeably with academic freedom.[36] This statutory obligation has been met by universities in various ways, including by referring to intellectual inquiry and academic freedom in institution-specific legislation, enterprise agreements, university policies, and codes of conduct.[37] The High Court of Australia has found, however, that such protections for intellectual freedom can be curtailed by university codes of conduct and enterprise agreements.[38]

---

[26] Ibid; Robert French, *Report of the Independent Review of Freedom of Speech in Australian Higher Education Providers* (Report, March 2019) 102 ('*French Review*'); Fred D'Agostino and Peter Greste, 'Slippery Beasts: Why Academic Freedom and Media Freedom are so Difficult to Protect' (2021) 63(1) *Australian Universities' Review* 45, 46–7.

[27] Evans and Stone (n 16) 53–4; Rob Watts, 'What Crisis of Academic Freedom? Australian Universities after French' (2021) 63(1) *Australian Universities' Review* 8, 15; D'Agostino and Greste (n 26) 47; Barendt (n 15) 50–63, 71.

[28] See *Human Rights Act 2004* (ACT) ('*ACT HRA*'); *Charter of Human Rights and Responsibilities Act 2006* (Vic) ('*Vic HRA*'); *Human Rights Act 2019* (Qld) ('*Qld HRA*').

[29] *Constitution of Japan* art 23.

[30] *Constitution of the Republic of South Africa Act 1996* (South Africa) art 16(1)(d).

[31] *Constitucion Española* [Constitution of Spain] art 20(1)(c).

[32] *Grundgesetz für die Bundesrepublik Deutschland* [Basic Law for the Federal Republic of Germany] art 5(3). For a comparative analysis of academic freedom, see Barendt (n 15).

[33] Academic freedom can also be found in the *International Covenant on Economic, Social and Cultural Rights*, to which Australia is a party: *International Covenant on Economic, Social and Cultural Rights*, opened for signature 16 December 1966, 993 UNTS 3 (entered into force 3 January 1976) art 15.

[34] See *Higher Education Support Act 2003* (Cth) s 19-115 ('*HESA*'). See also *Higher Education Standards Framework (Thresholds Standards) 2021* standard 6.1.4.

[35] Evans and Stone (n 16) 33–5; see *Higher Education Support Amendment (Freedom of Speech) Act 2021* (Cth) sch 1.

[36] *Ridd v JCU* (n 19) 22–3 [29]; Evans and Stone (n 16) 36–7. Although, at times intellectual freedom has been defined to be wider than academic freedom: Evans and Stone (n 16) 35–6; *Ridd v JCU* (n 19) 22–3 [29]; *James Cook University v Ridd* (2020) 278 FCR 566, 2588 [97] ('*JCU v Ridd*'). Additionally, the Federal Court of Australia has insisted that intellectual freedom and academic freedom are distinct: *JCU v Ridd* (n 36) 585 [90]; Evans and Stone (n 16) 36.

[37] Evans and Stone (n 16) 37–40. See, eg, *Ridd v JCU* (n 19) 17–19 [11]–[16]; *National Tertiary Education Industry Union v University of Sydney* (2021) 392 ALR 252, 276–81 [104]–[106] ('*Anderson*').

[38] See generally *Ridd v JCU* (n 19); *Anderson* (n 37).

In contrast to the nature of the protections for academic freedom, freedom of expression is protected under human rights Acts in Victoria, Queensland and the Australian Capital Territory (where each arm of government is required to act compatibly with the freedom).[39] However, the freedom is not absolute, but rather is subject to 'reasonable limits set by laws that can be demonstrably justified in a free and democratic society'.[40] While a general right to freedom of speech or expression is not protected in the *Australian Constitution*, a related freedom is: the implied freedom of political communication.[41] The implied freedom imposes limits on legislative power to prevent unjustifiable or disproportionate burdens on political communications.[42] Like the freedoms found in Australian human rights Acts, however, the implied freedom can be restricted where there is a legitimate objective for the law and the response is proportionate.[43]

Although the *HESA* now refers to 'freedom of speech and academic freedom' rather than 'free intellectual inquiry'[44] (a change that some scholars argued would better protect academic freedom),[45] these amendments still do not protect encroachments on academic freedom from outside the university (such as where Commonwealth laws criminalise certain research and teaching pursuits).[46] Although it could be argued that these kinds of encroachments would be better protected by including academic freedom in human rights Acts, those Acts suffer from their own limitations,[47] including that not all states and territories currently have such legislation.

As yet, academic freedom has 'no settled definition'.[48] Common elements can, however, be identified, with the scope of academic freedom flowing directly from its justifications.[49] Evans and Stone suggest that academic freedom consists of the freedom to research, the freedom to teach and learn, and institutional freedom.[50] These elements are reflected in the suggested definition of 'academic freedom' in the 2019 *French Review*'s proposed 'Model Code for the Protection of Freedom of Speech and Academic Freedom in Australian Higher Education Providers':

---

39 *ACT HRA* (n 28) s 16; *Vic HRA* (n 28) s 15; *Qld HRA* (n 28) s 21. Freedom of expression is also protected under the *International Covenant on Civil and Political Rights*, to which Australia is a party: *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 19.

40 *ACT HRA* (n 28) s 28(1); *Qld HRA* (n 28) s 13(1). Similarly, see *Vic HRA* (n 28) s 7(2).

41 Derived from *Australian Constitution* ss 7, 24, 64, 128.

42 See, eg, *Australian Capital Television Pty Ltd v Commonwealth* (1992) 177 CLR 106; *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520; *McCloy v New South Wales* (2015) 257 CLR 178; *Brown v Tasmania* (2017) 261 CLR 328.

43 Ibid.

44 *HESA* (n 34) s 19-115.

45 Evans and Stone (n 16) 36–7.

46 Indeed, the Australian Government has posed a significant threat to academic freedom in the past: ibid 31.

47 See, eg, Andrew Byrnes, Hilary Charlesworth and Gabrielle McKinnon, *Bills of Rights in Australia: History, Politics and Law* (University of NSW Press, 2007); Julie Debeljak, 'Balancing Rights in a Democracy: The Problems with Limitations and Overrides of Rights under the *Victorian Charter of Human Rights and Responsibilities Act 2006*' (2008) 32(2) *Melbourne University Law Review* 422.

48 *French Review* (n 26) 18. See also *JCU v Ridd* (n 36) 588 [97].

49 *French Review* (n 26) 18; Evans and Stone (n 16) 54.

50 Evans and Stone (n 16) 54–6.

- the freedom of academic staff to teach, discuss, and research and to disseminate and publish the results of their research;
- the freedom of academic staff and students to engage in intellectual inquiry, to express their opinions and beliefs, and to contribute to public debate, in relation to their subjects of study and research;
- the freedom of academic staff and students to express their opinions in relation to the higher education provider in which they work or are enrolled;
- the freedom of academic staff, without constraint imposed by reason of their employment by the university, to make lawful public comment on any issue in their personal capacities;
- the freedom of academic staff to participate in professional or representative academic bodies;
- the freedom of students to participate in student societies and associations; and
- the autonomy of the higher education provider in relation to the choice of academic courses and offerings, the ways in which they are taught and the choices of research activities and the ways in which they are conducted.[51]

This definition of academic freedom (with the exception of 'the freedom of academic staff … to make lawful public comment') has been included in the recently amended *HESA*.[52] The High Court of Australia has also discussed the elements of academic freedom, noting that free inquiry and participation and discussion in university governance are considered to be essential elements.[53] In this article, I use the above *French Review* elements of academic freedom to assess whether, and how, Australia's espionage laws impact on academic freedom.

In addition to considering the elements of academic freedom, the High Court noted the *French Review*'s observation that intellectual freedom is 'a defining characteristic of universities and like institutions'.[54] Due to the 'instrumental and ethical foundations'[55] for the freedom — and its 'long-standing core meaning'[56] — the freedom is 'not qualified by a requirement to afford respect and courtesy in the manner of its exercise'.[57] Despite giving academic freedom legal weight, the Court did emphasise that the freedom could be limited.[58] Evans and Stone have agreed with this, but they suggest that any limits should be minimal because of the

---

51 *French Review* (n 26) 230–1. These elements of academic freedom have also been discussed in, for example, Watts (n 27) 12–13.

52 *HESA* (n 34) sch 1, s 1(1) (definition of 'academic freedom'). This element was not included as it was considered to fit more appropriately within the 'broader societal freedom' of 'freedom of speech': Explanatory Memorandum, Higher Education Support Amendment (Freedom of Speech) Bill 2020 (Cth) 10.

53 *Ridd v JCU* (n 19) 23 [30].

54 Ibid, quoting *French Review* (n 26) 114.

55 *Ridd v JCU* (n 19) 24 [33].

56 Ibid 31 [64].

57 Ibid. See also Evans and Stone (n 16) 59, and *Anderson* (n 37) 315 [250] in the latter of which it was agreed that academic freedom does not include a requirement to be courteous.

58 *Ridd v JCU* (n 19) 23–4 [32]–[33], 24 [35].

importance of academic freedom (compared to the general freedom of speech).[59] They argue, for example, that the freedoms of research and teaching should be limited to research and teaching that draws on disciplinary expertise, respects disciplinary standards, and relates to specialised research.[60] These limitations still give academics wide latitude to conduct research and teaching.

Another appropriate limitation would be to restrict the freedom to teaching and research that is legitimate (that is, not engaged in for the purposes of criminal activity, including espionage). Within the confines of legitimate research and teaching endeavours, however, academics should be free to exercise their academic freedom. If Australia's espionage laws capture legitimate research and teaching activities, they necessarily undermine academic freedom and must be reformed so that the freedom is upheld. In the remainder of this article, I consider the impact of Australia's espionage laws on legitimate research and teaching by academics.

III Australia's Espionage Laws and Their Impact on Academic Teaching and Research

Before engaging in an analysis of Australia's espionage offences and their impact on the legitimate work of academics, I first provide an introduction to and overview of Australia's espionage framework.

In 2018, the Federal Government overhauled the four existing espionage offences and replaced them with a complex scheme of 27 entirely new offences.[61] These consist of 'underlying', 'aggravated' and 'espionage-related' offences, with penalties ranging from 15 years' to life imprisonment. The 2018 espionage scheme also included three defences.

In summary, the underlying offences include: the 'Core Espionage Offence',[62] 'Communication Espionage',[63] 'Classified Information Espionage',[64] 'Espionage on behalf of a Foreign Principal'[65] and 'Trade Secrets Espionage'.[66] Some of these offences have alternative fault elements — either intention or recklessness as to certain national security consequences — creating sub-offences for each underlying offence and, ultimately, a total of nine different underlying offences. Four aggravating circumstances apply to four of these underlying offences, creating 16 aggravated offences.[67] The espionage-related offences include soliciting espionage (the 'Solicitation Offence')[68] and preparing for espionage (the 'Preparatory Offence').[69]

---

59 Evans and Stone (n 16) 12–13.
60 Ibid 54–5.
61 See *Criminal Code* (n 7) divs 91, 92A.
62 Ibid s 91.1.
63 Ibid s 91.2.
64 Ibid s 91.3.
65 Ibid s 91.8.
66 Ibid s 92A.1. For a table summarising these offences and the penalties prescribed by the legislation, see Kendall, 'Australia's New Espionage Laws' (n 9) 143.
67 *Criminal Code* (n 7) s 91.6.
68 Ibid s 91.11.
69 Ibid s 91.12.

All of the espionage offences (with the exception of Trade Secrets Espionage) apply to conduct or results of conduct that occur within or outside Australia.[70] Trade Secrets Espionage applies only to conduct that occurs within Australia or, if the conduct occurs outside Australia: (i) where the result of the conduct occurs in Australia, or (ii) at the time of the offence, the person was an Australian citizen or resident.[71]

In Part III(A)–(E) below, I consider each of the espionage offences and defences and their relevance to academics. My analysis shows that five offences — the Core Espionage Offence, Communication Espionage, Espionage on behalf of a Foreign Principal, the Solicitation Offence and the Preparatory Offence — are of particular concern to academics and could erode academic freedom because they have the capacity to criminalise legitimate research and teaching. Despite this, available defences are inadequate.

A *Underlying Offences*

As described above, nine underlying espionage offences were introduced in 2018. At their core, each of these offences criminalise 'dealing' with 'information or an article' on behalf of, or to communicate to, a 'foreign principal'. Some of the offences also require an intention or recklessness as to certain 'national security' consequences. For some offences, national security also refers to the type of information or articles dealt with. These four key terms — dealing, information or articles, foreign principal, and national security — are central to defining espionage in Australia and largely set the boundaries of the kind of behaviour that is criminalised. There has been no judicial consideration of the terms as yet, given there has only been one recorded espionage case under Australian Federal law and this dealt with the 1914 espionage offence.[72] Therefore, definitions must be sourced from the *Criminal Code* and interpreted using principles of statutory interpretation.[73] In this section, I explain the key terms before considering each of the underlying offences in detail.

'Dealing' with information or an article means collecting, obtaining, making a record, copying, altering, concealing, communicating, publishing and making it available.[74] 'Make available' means: placing it somewhere it can be accessed by another person; giving it to an intermediary to give to a recipient; and describing how to obtain access to it or methods that are likely to facilitate access to it (for example, setting out a URL, password, or name of a newsgroup).[75] More broadly, however, 'deal' also includes merely receiving the information or article, or possessing it.[76]

---

70 Ibid ss 91.7, 91.10, 91.14, 15.4.
71 Ibid ss 92A.2, 15.2.
72 *R v Lappas* (2003) 152 ACTR 7. See Kendall, 'Australia's New Espionage Laws' (n 9) for a discussion of Australia's historical espionage laws.
73 See *Acts Interpretation Act 1901* (Cth).
74 *Criminal Code* (n 7) s 90.1(1) (definition of 'deal').
75 Ibid (definition of 'make available').
76 Ibid (definition of 'deal').

'Information' means 'information of any kind, whether true or false and whether in material form or not' and includes an opinion or report of a conversation.[77] This means that for the purposes of Australia's espionage framework, information includes anything from digital data and physical documents to untrue information about someone's opinion and a misrepresented report of a conversation between two people. 'Article' extends the operation of the espionage framework further to include 'any thing, substance or material'[78] and would include, for example, a sample of a new vaccine or a prototype of new technology. Dealing with information or an article includes dealing with all or part of it or dealing only with the 'substance, effect or description' of it.[79] For simplicity, I refer to 'information' instead of 'information or an article'.

Dealing with information is at the heart of what academics do. We obtain, alter, communicate, publish, and engage in other dealings with information (including expressing our own opinions on research) on a daily basis. This means that by the very nature of our work, academics are vulnerable to being captured by Australia's espionage laws. This makes other elements of the offences central to determining whether a crime has been committed by an academic.

The third key term, 'foreign principal', means a foreign government or authority (including a local government body), foreign political organisation, terrorist organisation, or an entity owned, directed or controlled by any foreign principal.[80] However, it also means a public international organisation or a foreign public enterprise.[81] Foreign public enterprises are companies, bodies or associations that enjoy special legal rights, status, benefits or privileges under the law of a foreign country because of their relationship with the foreign government.[82] The directors or executive committee members must also be accustomed to act according to the directions of the foreign government, or the foreign government must be in a position to exercise control over the company, body or association.[83] Alternatively, for companies alone, the government of the foreign country must hold more than 50% of the company's issued share capital or 50% of its voting power, or be in a position to appoint more than 50% of the board of directors.[84] This essentially means that foreign-owned or controlled entities are foreign principals for the purposes of Australian espionage law, provided they have some connection with a foreign government, authority or political organisation, or meet the requirements of a 'foreign public enterprise'.

Foreign (non-Australian) public universities or research organisations could be foreign principals under Australian espionage law, as 'foreign public enterprises' or entities 'owned, directed or controlled by' a foreign government. Public universities and research organisations are owned or funded by the state, and therefore could also be 'controlled' by the foreign government or be accustomed to

77 Ibid (definition of 'information').
78 Ibid (definition of 'article').
79 Ibid s 90.1(2).
80 Ibid ss 90.2, 90.3.
81 Ibid.
82 Ibid s 70.1 (definition of 'foreign public enterprise').
83 Ibid.
84 Ibid.

act according to the directions of the foreign government.[85] Some of these universities and research centres might even enjoy special legal rights, status, benefits or privileges as a result of their relationship with government, such as tax offsets or funding for infrastructure or student scholarships. Foreign public universities and research organisations that could be 'foreign principals' include, for example, China's top two civilian universities, Peking University[86] and Tsinghua University[87] (both funded and supervised by the Ministry of Education, among other state agencies), the United States' National Institutes of Health (part of the United States Department of Health and Human Services)[88] and University of California (funded by state and federal governments),[89] the United Kingdom's University of Manchester (funded by government)[90] and National Nuclear Laboratory (owned by government),[91] India's University of Delhi (funded by government),[92] and New Zealand's Crown Research Institutes (owned by the Crown).[93] I am not claiming here that these entities are engaging in espionage, however — I am merely illustrating the types of entities that may be 'foreign principals' under Australian law.

'National security', the final key term, has been defined to mean defence of the country; protection of the country from activities such as espionage, sabotage, terrorism, and foreign interference; and protection of the country's territory from serious threats.[94] However, the legislation also extends the meaning of national security beyond traditional defence matters to include the 'carrying out of the country's responsibilities to any other country' in relation to national security and 'the country's political, military or economic relations' with another country.[95] This essentially draws a country's international relations within the meaning of national security. The breadth of this definition has been criticised by the Senate Environment and Communications References Committee, who considered in its *Inquiry into Press Freedom Report* that 'the definition of the term "national security" departs from generally accepted interpretations of that term, resulting in the capture of topics

---

85 In the United States see, eg, American Academy of Arts & Sciences, *Public Research Universities: Understanding the Financial Model* (Report, February 2016).

86 Australian Strategic Policy Institute, 'Peking University', *China Defence Universities Tracker* (Web Page, 20 November 2019) <https://unitracker.aspi.org.au/universities/peking-university/>.

87 Australian Strategic Policy Institute, 'Tsinghua University', *China Defence Universities Tracker* (Web Page, 21 November 2019) <https://unitracker.aspi.org.au/universities/tsinghua-university/>.

88 'Who We Are', *National Institutes of Health* (Web Page, 2021) <https://www.nih.gov/about-nih/who-we-are>.

89 'The UC System', *University of California* (Web Page, 2021) <https://www.universityofcalifornia.edu/uc-system>.

90 Research England, '2019-20 Grant Tables for HEIs', *UK Research and Innovation* (Web Page, 2020) <https://re.ukri.org/finance/annual-funding-allocations/2019-20-grant-tables-for-heis/>.

91 'Corporate Information', *National Nuclear Laboratory* (Web Page, 2021) <https://www.nnl.co.uk/about/corporate-information/>.

92 'University and Higher Education', *Department of Higher Education* (Web Page, 19 February 2021) <https://www.education.gov.in/en/university-and-higher-education>.

93 'Crown Research Institutes', *Ministry of Business, Innovation and Employment* (Web Page, 6 January 2021) <https://www.mbie.govt.nz/science-and-technology/science-and-innovation/agencies-policies-and-budget-initiatives/research-organisations/cri/>.

94 *Criminal Code* (n 7) s 90.4.

95 Ibid s 90.4(1)(d)–(e).

that would otherwise be central to public discourse and journalism'.[96] The Committee recommended that the definition be reviewed, with particular consideration of how it could be amended to conform more closely with international law and jurisprudence.[97]

Now that we understand what these four key terms mean, we can look at each of the underlying espionage offences and examine whether they could capture legitimate research and teaching by academics. As a reminder, the underlying offences include: the Core Espionage Offence, Communication Espionage, Classified Information Espionage, Espionage on behalf of a Foreign Principal, and Trade Secrets Espionage. I will now discuss each of these offences in turn.

1 *The Core Espionage Offence*

The Core Espionage Offence criminalises dealing with security classified[98] or national security information that results or will result in the information being communicated or made available to a foreign principal or person acting on its behalf (although it is not necessary that the person have in mind a particular foreign principal).[99] The first sub-offence requires that the person must also intend for their conduct to prejudice Australia's national security or advantage the national security of a foreign country.[100] This sub-offence carries a maximum penalty of life imprisonment.[101] Alternatively, the second sub-offence carries a maximum penalty of 25 years' imprisonment and arises where the person is only reckless as to this prejudice or advantage.[102]

We know that academics deal with information. For the Core Espionage Offence to be enlivened, however, the dealing must result in communication to a foreign principal. The end product of academic research is usually publication in some form. Indeed, the *French Review* defined academic freedom to include the freedom of academics to 'disseminate and publish the results of their research' and to 'contribute to public debate'.[103] Furthermore, grants by the Australian Research Council and other agencies generally require research outputs to be made publicly available. Publication in any form — whether this be a journal article, book, conference paper or other publication — effectively places the research in the public domain to be accessed by anyone, including foreign principals. Even if the publication is intended for a specific audience, publication by its very nature means the work is generally available to the public at large. Where the publication is behind a paywall, it may still result in 'communication to a foreign principal' because all that is needed is payment — by any person — for access.

---

96 Senate Environment and Communications References Committee, Parliament of Australia, *Inquiry into Press Freedom* (Report, May 2021) 118–19 [7.29].

97 Ibid 119 [7.31].

98 Security classified information is information with a security classification of secret or top secret: *Criminal Code* (n 7) s 90.5.

99 Ibid ss 91.1(1), 91.1(4)(a).

100 Ibid s 91.1(1)(c).

101 Ibid s 91.1(1).

102 Ibid s 91.1(2).

103 *French Review* (n 26) 230–1.

However, communication to a foreign principal by academics can occur in ways other than publication too. In its submission to the PJCIS Inquiry, Universities Australia submitted that in 2018, 29% of university students (412,567 students) were international students.[104] Communication to a person acting on behalf of a foreign principal could, in theory, occur through teaching international students in class or providing information to them via online learning platforms, especially as 'information' extends to opinions.[105] I am not suggesting here that all international students are 'acting on behalf of a foreign principal', rather, I seek to demonstrate the breadth of conduct that could amount to communications to a foreign principal.

Such communications could also occur where academics collaborate with researchers employed by a foreign public university. As submitted to the PJCIS Inquiry by Universities Australia, 78% of Australia's most highly cited publications are attributed to international collaborations.[106] Australia's top international partners include China, the United States, the United Kingdom, Germany, the European Union and Canada.[107] As discussed above, foreign public universities may be foreign public enterprises or 'entities owned, directed or controlled by' a foreign principal. If research is shared with collaborators from such universities, this may certainly fall under 'communications to a person acting on behalf of a foreign principal'.

Since academics 'deal with information' daily and this will likely (or is intended to) result in 'communication to a foreign principal', whether or not their conduct satisfies all elements of the Core Espionage Offence therefore depends on two factors. First, the type of information dealt with and, second, the fault element. The Core Espionage Offence only applies when the person deals with security classified or national security information.[108] Academics do not often deal with classified information, but those that do are usually funded by Defence.[109] In circumstances such as these, however, the researchers involved are often aware of their obligations under the research partnership and know not to share their research beyond the bounds of what is contractually permitted.[110] If they do deal with their research contrary to their contract, this would be strong grounds for establishing that the person had the requisite mens rea (or fault element). The fault elements for the Core Espionage Offence will be discussed below.

While most academics do not deal with classified information, the same cannot be said for national security information. As described above, national

---

104 Universities Australia, Submission No 26 to PJCIS, *Inquiry into National Security Risks Affecting the Australian Higher Education and Research Sector* (December 2020) 3.

105 See above n 77 and accompanying text.

106 Universities Australia (n 104) 6.

107 Ibid 7; Group of Eight Australia, Submission No 34 to PJCIS, *Inquiry into National Security Risks Affecting the Australian Higher Education and Research Sector* (18 December 2020) 4.

108 *Criminal Code* (n 7) ss 91.1(1)–(2).

109 See, eg, Universities Australia (n 104) 10; Department of Defence (Cth), Submission No 42 to PJCIS, *Inquiry into National Security Risks Affecting the Australian Higher Education and Research Sector* (December 2020); CQ University, Submission No 3 to PJCIS, *Inquiry into National Security Risks Affecting the Australian Higher Education and Research Sector* (December 2020) 3.

110 See, eg, La Trobe University, Submission No 4 to PJCIS, *Inquiry into National Security Risks Affecting the Australian Higher Education and Research Sector* (December 2020) 2; Western Sydney University, Submission No 9 to PJCIS, *Inquiry into National Security Risks Affecting the Australian Higher Education and Research Sector* (16 December 2020) 5.

security not only includes defence and intelligence information, but also information on a country's economic and political relations.[111] The definition of national security is so broad that it would extend to all aspects of these areas, from current and historical organisational and governmental policies; national security laws; geopolitics, relations between states and actual or proposed treaties; and misconduct or corruption by defence, intelligence or government employees, through to defence and intelligence strategies, technologies, capabilities and training. This type of information is handled by academics from various disciplines, including political science, international relations, peace and conflict studies, law, criminology, history, geography and science, technology, engineering and mathematics ('STEM'). Any academic whose research involves this kind of information may therefore be at risk of committing the Core Espionage Offence. Whether or not they have in fact committed a criminal offence will, however, depend on proof of the fault element.

As described above, the Core Espionage Offence has two alternative fault elements, essentially creating two sub-offences. For the first sub-offence, the person must have *intended* either to prejudice Australia's national security or to advantage the national security of a foreign country.[112] For the second sub-offence, the person must have been *reckless* as to either of these things.[113] The *Criminal Code* defines intention to mean: the person means to engage in the conduct; they believe a circumstance exists or will exist; or they mean to bring about a result or are aware that it will occur in the ordinary course of events.[114] In contrast, recklessness criminalises a much lower level of personal culpability. A person is reckless if he or she is are aware of a substantial risk that the circumstance exists or that the result will occur and, having regard to the circumstances known to him or her, it is unjustifiable to take the risk.[115] Proving that an academic intended to prejudice Australia's national security, or to advantage the national security of another country, may be difficult owing to the relatively high level of personal culpability necessary to establish intention.[116] However, where an academic impermissibly dealt with classified information (a scenario posited above), this certainly may be sufficient to prove they meant for (intended) their actions to prejudice or advantage national security.

As a result of the legislative definitions of 'prejudice' and 'advantage', however, it is possible that an intention to prejudice or advantage national security could be established in other circumstances too. Prejudice and advantage have not been positively defined in the *Criminal Code*, making it unclear exactly what amounts to an intention (or recklessness) as to prejudice or advantage. 'Prejudice' has been defined to mean only that 'embarrassment alone is not sufficient to *prejudice* Australia's national security'[117] while 'conduct will not *advantage* the national security of a foreign country if the conduct will advantage Australia's

111 *Criminal Code* (n 7) s 90.4. See above nn 94–6 and accompanying text.
112 Ibid s 91.1(1).
113 Ibid s 91.1(2).
114 Ibid s 5.2.
115 Ibid s 5.4.
116 Ibid s 5.2.
117 Ibid s 90.1(1) (definition of 'prejudice') (emphasis in original).

national security to an equivalent extent'.[118] Prejudice, therefore, would encompass an intention to harm Australia's national security in some way, but may also extend to, for example, an intention to reveal government misconduct or portray Australia in a bad light on the international stage — so long as this is more than mere embarrassment.[119] The definition of advantage is equally perplexing. It could encompass an intention to advantage the national security of a foreign country but only have a neutral effect on Australia. Or, it could arise where the person intended their conduct to advantage Australia's national security to an extent, but not so much that it is equivalent to the foreign country's advantage.

The uncertainty of these terms has implications for the scope of the Core Espionage Offence (as well as other underlying offences which utilise these terms) — the fault elements may be wide enough to capture the legitimate work of academics. For example, it may be sufficient to prove an academic intended to prejudice Australia's national security — and therefore that they committed the Core Espionage Offence — where they engaged in a research project that resulted in criticism of Australian military or intelligence policies or practices, or that catalogued Australian Government misconduct in treaty negotiations or relations with other countries. Since the Core Espionage Offence only requires that the dealings 'will result in communication to a foreign principal',[120] any steps towards publication of this kind of information (and not just the publication itself) could also be a crime: that is, any part of the research process, including merely developing research questions (especially if these are framed to show the Government in a bad light). An intention to advantage another country's national security, on the other hand, could arise where, for example, an Australian academic collaborating with an academic from the University of Delhi publishes research on new technology that has a defence application, where Australia already has similar (but not quite as good) technology in use, but India does not have that technology at all. In this scenario, as foreign public universities can be foreign principals, even just communications with the academic's Indian counterpart about the project (prior to publication) could amount to the Core Espionage Offence.

The alternative fault element for the Core Espionage Offence — recklessness as to prejudice or advantage — will be easier to prove than intention and could significantly broaden the offence's scope. Where academics research topics that are clearly of a sensitive nature, such as dual-use technologies or projects, policies or strategies for national security organisations and/or national defence, this may easily be enough to show there is a 'substantial risk' of prejudice or advantage to national security. So, an academic working on the development of a new supersonic missile who shares information about the project on social media would certainly have been

---

118 Ibid (definition of 'advantage') (emphasis in original).

119 Arguably, Witness K's revelations about government misconduct during treaty negotiations would have satisfied this element. Witness K revealed to his security cleared barrister, Bernard Collaery, secret information that Australian Secret Intelligence Service agents had bugged the Timor-Leste government offices during oil and gas treaty negotiations: see, eg, Christopher Knaus, 'Witness K and the "Outrageous" Spy Scandal that Failed to Shame Australia' *The Guardian* (online, 10 August 2019) <https://www.theguardian.com/australia-news/2019/aug/10/witness-k-and-the-outrageous-spy-scandal-that-failed-to-shame-australia>.

120 *Criminal Code* (n 7) s 91.1(d).

reckless (and have committed the Core Espionage Offence). But so too might an academic who publishes an article on (or begins research into) the approach of the Australian Security Intelligence Organisation ('ASIO') to monitoring suspected terrorists or spies. Where the research involves less sensitive information, it may still be possible to prove recklessness because of the breadth of 'national security'. For example, an academic may be aware that there is a risk that a project investigating Australia's relations with Indonesia will benefit Indonesia's economy or military, or that research into Australian national security laws will result in criticism of those laws. In each scenario, the academics involved may well have broken the Core Espionage Offence. In all the scenarios described so far, the academics might even have committed a crime just by talking about their research in class (if international students were present) or by communicating with colleagues if they were collaborating with a foreign public university.

Ultimately, the Core Espionage Offence poses a real risk to academics working on projects involving sensitive or classified information, or anything related to traditional conceptions of national security, as well as academics working on international relations projects (especially where this could reveal something bad about Australia (beyond embarrassment) or benefit another country). What is important is not how the project is carried out (that is, the methods used), but the topic investigated and how it has been framed. By criminalising the work of these academics, important research may be avoided or stifled, contributing to the erosion of academic freedom.

2 *Communication Espionage*

Like the Core Espionage Offence, Communication Espionage criminalises dealings with information where this results or will result in communication to a foreign principal.[121] However, it places no limit on the type of information dealt with — the information may be of any kind — so it applies to a broader range of conduct. It is therefore limited only by its fault element. This makes Communication Espionage a greater threat to academics — and academic freedom — than the Core Espionage Offence.

There are two fault elements for Communication Espionage, creating two sub-offences: intention to prejudice Australia's national security (which carries a maximum penalty of 25 years' imprisonment),[122] or recklessness as to this (which carries a maximum penalty of 20 years' imprisonment).[123] Unlike the Core Espionage Offence, there is no alternative fault element prescribing an intention (or recklessness) as to advantaging the national security of a foreign country. As described above, each of the two fault elements has the potential to be proved in relation to the work of certain academics — those most at risk are academics working with classified, sensitive, national security or international relations information (especially where their research critiques Australia). However, because the offence is not restricted to classified or national security information, it could

[121] Ibid s 91.2.
[122] Ibid s 91.2(1).
[123] Ibid s 91.2(2).

apply to any academic who is involved in a project that might prejudice Australia's national security (as broadly as it has been defined), even if they have only handled innocuous (non-classified/national security) information.

3 *Classified Information Espionage*

In contrast to Communication Espionage, Classified Information Espionage applies only to dealings with classified information.[124] In addition to the requirement that the person's conduct results or will result in communication of the information to a foreign principal, the person must deal with the information for the primary purpose of communication to a foreign principal.[125] There is no further fault element in relation to prejudice or advantage to national security.

In essence, the primary purpose of the job of academics is to generate and disseminate information. We do not just research — an important aspect of academic work is publication or dissemination in some way of the results of our research to the public and relevant stakeholders. As foreign principals are part of the wider public, the very nature of our work means it could be argued that academics have a primary purpose of communication to a foreign principal at every stage of the research process.

As such, Classified Information Espionage is limited by one factor alone — the type of information dealt with (classified information).[126] As discussed previously, not all academics' research involves classified information, but some does. These academics should already be well aware of their obligations regarding the handling of that information, including that they could commit an offence if they share details of their research in an unauthorised manner. As a result, it is unlikely that they will commit Classified Information Espionage inadvertently. This offence, therefore, poses less of a risk to academics, but those academics that do work with classified information should be aware that any unauthorised dealings may certainly constitute Classified Information Espionage, making them liable to up to 20 years' imprisonment.

4 *Espionage on behalf of a Foreign Principal*

Espionage on behalf of a Foreign Principal is a tiered collection of sub-offences whose maximum penalties are 15 years', 20 years' and 25 years' imprisonment.[127] For all sub-offences, the person must deal with information and this must be on behalf of, in collaboration with, or directed, funded or supervised by a foreign principal.[128] The person must also be reckless as to whether their conduct involves the commission of an espionage offence (by themselves or any other person).[129] This

---

124 Ibid s 91.3.
125 Ibid.
126 Ibid s 91.3(1)(c).
127 Ibid s 91.8.
128 Ibid ss 91.8(1), (2), (3).
129 Ibid.

is all that is required to prove the least serious of these sub-offences.[130] If the person is reckless as to whether their conduct will prejudice Australia's national security or advantage the national security of a foreign country[131] or, more seriously, they intend one of these national security consequences,[132] they will be liable to the higher maximum penalties.

The Espionage on behalf of a Foreign Principal offences are directed towards activities engaged in on behalf of a foreign principal, rather than dealings that result in communication to a foreign principal. The offences are therefore most applicable to academics collaborating with, or working for, foreign public universities or research organisations (where these constitute foreign public enterprises or entities 'owned, directed or controlled' by a foreign principal).[133]

Whether or not an academic has committed Espionage on behalf of a Foreign Principal depends on one, or potentially two, fault elements (reflecting which of the three sub-offences is being prosecuted). All three sub-offences require the person to have been reckless as to whether an espionage offence was being committed.[134] Thus, whether this element is established depends on proof that the person was aware of a substantial risk that they (or another person) would be committing espionage and acted despite it being unjustifiable to have done so.[135] This requires consideration of the circumstances of the case, including the type of information dealt with (for example, classified, sensitive or innocuous) and the organisation the person (or their collaborator) works for (for example, is it directed or controlled by a country that poses a threat to Australia or is an ally). If the academic was researching sensitive matters relating to Australia's national security policies or working on development of Defence capabilities and they were collaborating with someone working for China's Peking University, for example,[136] this may be sufficient to prove the person was being reckless as to the commission of an espionage offence. This contrasts with collaborative research into, for example, Australia's relations with New Zealand by academics from each of these countries, as these academics are unlikely to be aware that this would pose a risk of committing an espionage offence.

For the sub-offence carrying a maximum penalty of 15 years' imprisonment, this is all that needs to be established.[137] The other two sub-offences (carrying a maximum penalty of 25 and 20 years' imprisonment) have an additional fault element: the person must either intend to[138] or be recklessness as to whether they would prejudice Australia's national security or advantage the national security of a

130 Ibid s 91.8(3). This offence has a maximum penalty of 15 years' imprisonment.
131 Ibid s 91.8(2). This offence has a maximum penalty of 20 years' imprisonment.
132 Ibid s 91.8(1). This offence has a maximum penalty of 25 years' imprisonment.
133 See above nn 80–93 and accompanying text.
134 *Criminal Code* (n 7) ss 91.8(1)(c), 91.8(2)(c), 91.8(3)(b).
135 Ibid s 5.4.
136 While Australian security agencies have declined to name countries that pose a threat to Australia, many people think that China is one of the biggest threats: see, eg, Paul Maddison, 'Is China or Climate Change the Bigger Threat to Australia?', *The Strategist* (online, 2 December 2021) <https://www.aspistrategist.org.au/is-china-or-climate-change-the-bigger-threat-to-australia/>.
137 *Criminal Code* (n 7) s 91.8(3).
138 Ibid s 91.8(1)(b).

foreign country.[139] As discussed in relation to the Core Espionage Offence, both intention and recklessness could be proved in the context of academic research.[140] These two sub-offences are more likely to capture the conduct of academics researching sensitive, national security or international relations topics (particularly where this could show Australia in a bad light). So, the offences could arise where a project resulting in criticism of Australian intelligence alliances is engaged in by an Australian academic and their Chinese academic collaborator — as could any of the scenarios discussed so far where they involve a collaboration between an Australian academic and a foreign public university or research organisation (or employment by such organisations).

The Espionage on behalf of a Foreign Principal offences therefore create a real risk of criminalising the work of some academics who collaborate with or work for foreign public universities or research organisations. This may lead to the chilling of such international research collaborations and, ultimately, the stifling of academic freedom globally.

5 *Trade Secrets Espionage*

Trade Secrets Espionage carries a maximum term of imprisonment of up to 15 years[141] and criminalises the dishonest dealing with trade secrets on behalf of, in collaboration with, or where directed, funded or supervised by a foreign government principal.[142] While 'foreign principal' is defined to include 'foreign government principal', the latter term is slightly narrower than the former, encompassing only foreign governments and their authorities, foreign public enterprises, and entities owned, directed or controlled by a foreign government principal.[143] Despite this narrower application, like Espionage on behalf of a Foreign Principal, the offence still applies to academics collaborating with or working for foreign public universities or research organisations.

As with the Core Espionage Offence and Classified Information Espionage, Trade Secrets Espionage applies only to a certain kind of information: trade secrets.[144] Trade secrets arise where:

> (i) the information is not generally known in trade or business, or in the particular trade or business concerned;
>
> (ii) the information has a commercial value that would be, or could reasonably be expected to be, destroyed or diminished if it were communicated;
>
> (iii) the owner of the information has made reasonable efforts in the circumstances to prevent the information becoming generally known…[145]

---

139 Ibid s 91.8(2)(b).
140 See above nn 112–20 and accompanying text.
141 *Criminal Code* (n 7) s 92A.1.
142 Ibid s 92A.1.
143 Ibid s 90.3. See also above nn 80–1 and accompanying text.
144 Ibid s 92A.1.
145 Ibid s 92A.1(1)(b).

This could include, for example, the development of a new vaccine or quantum technology. It is not necessary for the trade secrets to be classified or relate to national security, which makes the offence applicable to a wider scope of information — and, therefore, to more academics — than some of the other underlying espionage offences.

To be Trade Secrets Espionage, however, the trade secrets must have been dishonestly received, obtained, taken, copied, duplicated, sold, bought or disclosed.[146] While the offence has no fault element as to national security consequences, this 'dishonest' element aims to ensure only improper conduct falls within the offence, and legitimate conduct is protected. The offence is therefore most likely to capture genuine espionage and does not pose much of a risk to academics (despite applying to a wider scope of research).

B *Aggravated Offences*

Aggravated espionage offences operate to increase the maximum penalty available where certain underlying offences are committed under circumstances of aggravation. The aggravations only apply to the Core Espionage Offence (where the fault element is recklessness), Communication Espionage (for fault elements of intention and recklessness) and Classified Information Espionage.[147] Aggravated circumstances include: dealing with information from a foreign intelligence agency; dealing with five or more security classified records; altering a record to remove or conceal its security classification; and at the time the information was dealt with, the person held an Australian Government security clearance.[148] Where these circumstances are made out, the maximum penalty available is increased from 20 years' to 25 years' imprisonment, or from 25 years' to life imprisonment.[149]

Of the four aggravations, only two are likely to apply to academics: first, the person dealt with five or more security classified records, and second, at the time they dealt with the information, the person held an Australian Government security clearance.[150] These aggravated circumstances will only apply to those academics working on security classified research. As already discussed, these researchers should be well aware of their obligations in relation to their research, making it less likely that they would inadvertently commit an espionage offence. If these academics do handle information contrary to what is permitted, however, this will be strong grounds for proving the requisite fault element of the Core Espionage Offence or Classified Information Espionage. Therefore, these academics should be warned that if they do mishandle information, not only are they at great risk of being prosecuted for an espionage offence, but they might also have committed an aggravated offence if they mishandled five or more classified records or held an Australian Government security clearance — making them liable to much higher maximum penalties.

146 Ibid s 92A.1(1)(a).
147 Ibid s 91.6(1)(a).
148 Ibid s 91.6(1)(b).
149 Ibid s 91.6(1).
150 Ibid ss 91.6(1)(b)(iii), 91.6(1)(b)(v).

C *Espionage-Related Offences*

The 2018 espionage reforms included, for the first time, two espionage-related offences: the Solicitation Offence and the Preparatory Offence. Both significantly widen the scope of conduct criminalised as espionage and carry maximum penalties of 15 years in prison.[151] Also, they both can be committed where an espionage offence is never committed or cannot be committed, and even if the person does not have in mind a particular dealing.[152]

1 *The Solicitation Offence*

The Solicitation Offence criminalises conduct engaged in with the intention of soliciting or procuring, or making it easier to solicit or procure, another person ('the target') to commit espionage.[153] It therefore focuses on the conduct of the person soliciting, not the person actually (or potentially) committing espionage. The conduct must, however, be done on behalf of, in collaboration with, or be directed, funded or supervised by a foreign principal or person acting on its behalf.[154] Therefore, like Espionage on behalf of a Foreign Principal and Trade Secrets Espionage, the offence would only apply to academics who collaborate with or are employed by foreign public universities or research organisations.

Despite this, the Solicitation Offence captures *any* conduct in relation to the target.[155] This makes the physical element of the offence exceptionally broad — it could apply to any aspect of the work of academics (including preliminary research, discussions with colleagues, and data analysis). It also means that the fault element (an intention to solicit or procure) is the crucial limiting factor when it comes to whether the offence captures academics, especially as it is not necessary for the target to actually or potentially be able to commit espionage.[156] Whether or not this intention can be proved turns on a range of contextual factors, including: the research area (does it involve classified or sensitive Australian information?); the foreign public university or research organisation involved (is it controlled/funded by a country that is considered a security threat to Australia?); and the type of information that the target (here, a potential or actual collaborator) has access to or researches (again, is this classified or sensitive Australian information?). For example, this offence could be engaged where an academic employed by Tsinghua University seeks to collaborate with or otherwise reaches out to an Australian researcher working on a project involving defence technologies, intelligence policies or Australia's economic relations with other countries (or vice versa).

Due to the breadth of conduct captured by the Solicitation Offence, the fault element is the only factor standing between the criminalisation — or protection — of genuine research collaborations on, and inquiries into, projects that may involve

---

151 Ibid ss 91.11(1), 91.12(1).
152 Ibid ss 91.11(3), 91.12(3).
153 Ibid ss 91.11(1)(a)–(b).
154 Ibid s 91.11(1)(c).
155 Ibid s 91.11(1).
156 Ibid s 91.11(3).

information on Australia's national security or international relations. In some cases, the circumstances of the collaboration may suggest that the academic/s seeking the collaboration had the requisite intention, enabling police to lay charges. Academics working for foreign public universities or research organisations must therefore exercise great caution when seeking to collaborate or work with academics who are working on Australian national security-related projects as they may find that their actions — from researching potential collaborators to drafting co-authored articles for publication — contravene the Solicitation Offence. Of all of Australia's espionage offences, the Solicitation Offence has the greatest potential to chill international research collaborations, contributing to the erosion of academic freedom in Australia and around the world.

2 *The Preparatory Offence*

The second espionage-related offence, the Preparatory Offence, is the most far-reaching of all of Australia's espionage laws. It makes it a crime for a person to engage in any conduct with the intention of preparing for, or planning, an espionage offence.[157] This offence effectively criminalises the earliest stages of a potential crime[158] — any 'preparations' (for example, Google searches, purchasing technology or telephoning a person) — when an espionage offence may never actually be committed or the conduct may ultimately have an innocent explanation.[159] The offence closely resembles the 'catch-all'[160] 'preparing for a terrorist act' offence found in s 101.6 of the *Criminal Code*, which has regularly been utilised in terrorism prosecutions.[161]

Like the Solicitation Offence, the Preparatory Offence criminalises *any* conduct.[162] The only limitation to this offence is the fault element — an intention to prepare for or plan an espionage offence.[163] The physical element of this offence ('conduct') is so broad that it could capture almost every aspect of the work of academics, from conducting preliminary research into potential projects, communicating with potential collaborators, and developing research questions, to collecting and analysing data, and drafting publications. Of course, engaging in the

157 Ibid ss 91.12(1)(a)–(b).

158 In the terrorism context see, eg, Andrew Lynch, Nicola McGarrity and George Williams, *Inside Australia's Anti-Terrorism Laws and Trials* (NewSouth, 2015) 31–4; George Williams, 'A Decade of Australian Anti-Terror Laws' (2011) 35(3) *Melbourne University Law Review* 1136, 1154; Edwina MacDonald and George Williams, 'Combatting Terrorism: Australia's *Criminal Code* Since September 11, 2001' (2007) 61(1) *Griffith Law Review* 27, 34.

159 *Criminal Code* (n 7) s 91.12(3).

160 Lynch, McGarrity and Williams (n 158) 29.

161 See, eg, Jessie Blackbourn and Nicola McGarrity, 'Prosecutions', *Australian National Security Law* (Web Page, 8 February 2017) <https://ausnatsec.wordpress.com/prosecutions/>; Williams (n 158) 1153. For more on the preparatory terrorism offence see Tamara Tulich, 'A View Inside the Preventive State: Reflections on a Decade of Anti-Terror Law' (2012) 21(1) *Griffith Law* Review 209; Tamara Tulich, 'Prevention and Pre-Emption in Australia's Domestic Anti-Terrorism Legislation' (2012) 1(1) *International Journal for Crime and Justice* 52. For a comparison of the preparatory terrorism and preparatory espionage offences, see Kendall, 'Australia's New Espionage Laws' (n 9) 153–6.

162 *Criminal Code* (n 7) s 91.12(1).

163 Ibid ss 91.12(1)(b), (3).

physical element alone will not be a criminal offence — there must be proof of intention. However, the Preparatory Offence is clearly broad, putting the work of academics at risk of being criminalised in the absence of added safeguards.

While 'intention' is meant to set a high bar for proving the fault element attached to this offence,[164] the type of research some academics do means that it may not be difficult to point to circumstances that could suggest the person had the requisite intention. These circumstances include: the area or topic that they research (intention is more likely to be proved where they research an area related to Australia's 'national security', as it is broadly defined); the tone of their research (for example, do they criticise the Australian Government or show Australia in a bad light?); and who they have had contact with (for example, have they contacted someone from a foreign public university (especially one located in a country which is not an Australian ally), or has a foreign researcher sought out an Australian working on a national security project?). An intention to prepare for espionage could be shown, for example, where an Australian academic plans to begin a project analysing suspect surveillance practices by ASIO and the Australian Signals Directorate. In this scenario, the Preparatory Offence could be engaged where the academic conducts preliminary research into the topic, even if they ultimately choose not to proceed with the project. The Preparatory Offence could similarly capture a foreign academic who takes any step towards collaborating with an Australian researcher on a project investigating practices of the Five Eyes Intelligence Alliance.[165]

In essence, the Preparatory Offence could capture the conduct of academics and researchers, like conversations or Google searches, far before commission of any act actually constituting espionage. Although the offence is useful for giving police the power to intervene before genuine espionage is committed, in the higher education sector it may stifle the freedom of academics to pursue what may be important intellectual inquiries.

3 *General Inchoate Liability and the Espionage-Related Offences*

The espionage-related offences are arguably the most far-reaching of Australia's espionage laws. However, the breadth of these laws is extended even further through application of general inchoate liability. In addition to substantive criminal offences, the *Criminal Code* contains inchoate liability provisions that extend criminal responsibility beyond the actual commission of a crime (therefore, they are named 'pre-crimes'[166]) — much like the espionage-related offences themselves. These provisions include: attempt;[167] aiding, abetting, counselling and procuring;[168] joint

---

[164] Ibid s 5.2.

[165] This alliance — forged through the UKUSA Agreement — requires Australia, the United Kingdom, the United States, Canada and New Zealand to share intelligence information: see, eg, Andrew O'Neil, 'Australia and the "Five Eyes" Intelligence Network: The Perils of an Asymmetric Alliance' (2017) 71(5) *Australian Journal of International Affairs* 529.

[166] See generally Andrew Ashworth and Lucia Zedner, *Preventive Justice* (Oxford University Press, 2014) ch 5.

[167] *Criminal Code* (n 7) s 11.1.

[168] Ibid s 11.2.

commission;[169] commission by proxy;[170] incitement;[171] and conspiracy.[172] Where found guilty of one of these inchoate offences (except incitement), the person is liable to the same punishment as if they had committed the actual offence (in the context of the espionage-related offences, 15 years' imprisonment).[173]

Each of these inchoate provisions (except attempt) applies to the Solicitation and Preparatory Offences.[174] This creates offences that are another step removed from the commission of a substantive crime (so they have been termed 'pre-pre-crimes'[175]). These kinds of offences are both complex and exceptionally broad. For example, it could be an offence to procure or incite someone to solicit someone else to commit espionage. This would criminalise conduct that occurs at least two stages prior to the commission of a possible espionage offence, and proof of such an offence would involve complex layering of different physical and fault elements.

Of the inchoate liability provisions, the attachment of conspiracy to the Solicitation and Preparatory Offences is most concerning as it has the capacity to criminalise the very early stages of a potential research project or collaboration.[176] Conspiracy arises where two or more people enter into an agreement, intending to commit an offence, and at least one person commits an overt act pursuant to the agreement.[177] Like the espionage-related offences, conspiracy can arise even where committing the offence is impossible.[178] It could effectively criminalise mere 'talk', where a precise plan has not yet been developed or attempted and the people involved never go on to commit an offence.[179] While conspiracy offences are useful because they give law enforcement the power to intervene far before a serious crime has been committed, they can be problematic where the substantive offence/s to which they attach are overly broad. This is because such offences criminalise agreements to engage in conduct that arguably should not be a criminal offence in the first place.

For example, two academics may have conspired to prepare for espionage if they discussed a potential research project on Australian military war crimes, even if they decided not to pursue the project. Conspiracy to solicit espionage may arise where those academics suggest reaching out to an expert on Australian military affairs, where one or both of the academics work for a foreign public university. In each of these scenarios, the academics involved could face up to 15 years in prison for engaging in routine research activities.[180] These offences may seem far-fetched,

169 Ibid s 11.2A.
170 Ibid s 11.3.
171 Ibid s 11.4.
172 Ibid s 11.5.
173 Ibid ss 11.1(1), 11.2(1), 11.2A(1), 11.3(1), 11.5(1). For incitement, the person is liable to up to 10 years' imprisonment: ibid s 11.4.
174 Ibid ss 91.11(4), 91.12(2).
175 See generally Ashworth and Zedner (n 166) ch 5; Williams (n 158) 1155.
176 In the terrorism context, see Lynch, McGarrity and Williams (n 158) 39.
177 *Criminal Code* (n 7) s 11.5(2).
178 Ibid s 11.5(3).
179 Lynch, McGarrity and Williams (n 158) 39.
180 *Criminal Code* (n 7) s 91.12(1).

but conspiracy to prepare has been used frequently in the terrorism context and been responsible for prison sentences of up to 28 years.[181]

Pre-pre-crimes not only create complex derivative offences, but significantly extend the criminal law beyond its traditional bounds, criminalising conduct that may only have the potential to cause harm in some other way or that is, in itself, harmless (such as the everyday work of academics).[182] While indirect harms can be legitimate targets for the criminal law, the scope of these espionage-related offences takes the espionage pre-pre-crimes far beyond other legitimate examples (such as conspiring to commit a terrorist act[183]). As a result, they are likely to undermine, not uphold or preserve, the constitutionally prescribed system of democratic government, including by eroding academic freedom.

D *Defences*

Three defences were included in Australia's 2018 espionage reforms, but not all apply to every espionage offence (and none apply to Trade Secrets Espionage — although this is not so problematic in the present context as this offence is less likely to apply to academics). The first defence — 'Lawful Dealing' — arises where the person dealt with the information according to a Commonwealth law or agreement, or in their capacity as a public official.[184] However, it is unlikely to arise in circumstances where academics have been caught by the espionage offences. While it might be relevant where an academic working on a classified project handled the information according to the terms of their contract, this conduct, in itself, would not be sufficient to trigger any of the espionage offences.

The second defence — 'Authorised Prior Publication' — protects persons who dealt with information that was already communicated to the public with the authority of the Commonwealth.[185] It applies to all offences except Trade Secrets Espionage and the espionage-related offences. This defence might be relevant where academics' research involves national security information provided to the public via government sources (such as ASIO's Annual Threat Assessment or the Australian Federal Police's Annual Report). Academics do not always rely on government-sourced information, however. Indeed, an important aspect of their job can be gathering research from independent sources, such as the media and relevant stakeholders. In these circumstances, even though the information might have been made public, if it was not authorised by the Commonwealth then the defence cannot apply.

---

181 Lynch, Williams and McGarrity (n 158) 94–7; Nicola McGarrity, '"Testing" Our Counter-Terrorism Laws: The Prosecution of Individuals for Terrorism Offences in Australia' (2010) 34(2) *Criminal Law Journal* 92, 125–6.

182 See, eg, McGarrity (n 181) 114; Peter Ramsay, 'Democratic Limits to Preventive Criminal Law' in Andrew Ashworth, Lucia Zedner and Patrick Tomlin (eds), *Prevention and the Limits of the Criminal Law* (Oxford University Press, 2013) 214, 216; Jude McCulloch, 'Human Rights and Terror Laws' (2015) 128 *Precedent* 26, 28–9; Daniel Ohana, 'Responding to Acts Preparatory to the Commission of a Crime: Criminalization or Prevention?' (2006) 25(2) *Criminal Justice Ethics* 23, 28.

183 *Criminal Code* (n 7) ss 101.6(1), 11.5.

184 Ibid ss 91.4(1), 91.9(1), 91.13.

185 Ibis ss 91.4(2), 91.9(2).

The third defence, while the broadest of available defences, has limited application. 'Unauthorised Prior Publication' applies only to Classified Information Espionage and the Core Espionage Offence (where the prosecution relies on the fault element of advantage to the national security of a foreign country).[186] The defence arises where the information was already communicated to the public — so might be relevant where the academic re-published information that was already in the public domain.[187] It does not, however, apply where the person obtained the information as a result of them being engaged to work for the Commonwealth (so would rule out any academics working with or for government departments), or where they were involved in the prior publication.[188]

For the defence to arise, it is also necessary that the person had reasonable grounds for believing that dealing with the information would not prejudice Australia's national security, having regard to the nature, extent and place of prior publication.[189] Whether or not this can be proved may turn on the nature of the information itself (for example, whether it is classified, sensitive, related to international relations, or innocuous) and where it was initially published. If classified information revealing Australian military war crimes was published on national media,[190] further re-publication of this information in an academic journal article may not reasonably prejudice Australia's national security, given any prejudice would have already occurred. In contrast, publication of such information in a leading Australian political science journal — where it was originally published on a blog with a small readership — may demonstrate an unreasonable belief with respect to further prejudice.

While the Authorised Prior Publication and Unauthorised Prior Publication defences may protect some academics, they only apply to selected espionage offences — neither defence applies to the Solicitation and Preparatory Offences, while only Authorised Prior Publication (which is limited in scope) applies to Communication Espionage, Espionage on behalf of a Foreign Principal and the Core Espionage Offence (for the fault element of prejudice to Australia's national security). Furthermore, there is no defence for academics that use research that was not previously published, such as data from interviews or surveys — yet this kind of research is frequently conducted. Ultimately, therefore, the defence framework inadequately protects academics, leaving them vulnerable to prosecution for pursuing academic endeavours that may be of great benefit to Australian society and beyond.

---

186 Ibid s 91.4(3).
187 Ibid.
188 Ibid.
189 Ibid.
190 This occurred in 2017 when investigative journalists Dan Oakes and Sam Clark published 'The Afghan Files', a report based on leaked classified information that alleged that members of the Australian Defence Force had committed severe human rights violations in Afghanistan: see Dan Oakes and Sam Clark, 'The Afghan Files', *ABC News* (online, 11 July 2017) <https://www.abc.net.au/news/-07-11/killings-of-unarmed-afghans-by-australian-special-forces/8466642?pfmredir=sm&nw=0>. These allegations have since been investigated and substantiated: see Paul Brereton, *Inspector-General of the Australian Defence Force Afghanistan Inquiry Report* (Report, 10 November 2020).

E *Attorney-General's Consent*

It is worth noting here that proceedings for committing a person for trial for an espionage offence cannot be commenced without the Federal Attorney-General's consent.[191] This requirement is intended to act as a safeguard against prosecutions of non-genuine espionage. Indeed, Director-General of ASIO, Mike Burgess, has stated that 'we do not investigate journalists for their journalism, academics for their research or politicians for their politics'.[192] While the consent provision does provide an additional layer of protection for academics, it also raises a number of serious concerns. Most notably, the Government is essentially asking us to trust that it will not give its consent when legitimate conduct is concerned. If the laws capture such conduct, but the Government insists that it will not be prosecuted, then what is the point of having such over-expansive legislation? It is not hard to imagine that the Government might want to retain the wide-reaching laws just in case there ever comes a time when it thinks it would be appropriate to prosecute an academic (or other person engaged in legitimate activities, such as journalists). Even if this is not the case, the current Government cannot speak for future governments — there could be a time when a future Attorney-General consents to the prosecution of an academic for pursuing research simply because the Government does not want that research pursued.

This raises another problematic aspect of the consent provisions — they cannot help but politicise the prosecutorial process. Indeed, this was something that arguably occurred in the prosecution of Bernard Collaery and Witness K.[193] The Commonwealth Director of Public Prosecutions requested the consent of Attorney-General George Brandis to prosecute Collaery and Witness K in 2015.[194] This consent was not given until 2017, after Christian Porter was sworn in as Attorney-General.[195]

Furthermore, even though the Attorney-General's consent is needed to commit a person to trial, the *Criminal Code* still permits the person to be arrested and charged, and for a search warrant to be executed, without the Attorney-General's consent.[196] This in itself, as well as the uncertainty over whether the Attorney-General will in fact consent to prosecutions, may deter some academics from pursuing certain intellectual inquiries (like those that might result in criticism of the Government), chilling research into these areas and, ultimately, eroding academic freedom.

---

191 *Criminal Code* (n 7) s 93.1(1).

192 Mike Burgess, 'Director-General's Annual Threat Assessment', *ASIO* (Transcript, 17 March 2021) <https://www.asio.gov.au/resources/speeches-and-statements/director-generals-annual-threat-assessment-2021>.

193 See above n 119.

194 See Steve Cannane, 'Government Sat on Witness K Prosecution for Years Despite Advice', *ABC News* (online, 6 October 2018) <https://www.abc.net.au/news/2018-10-06/government-sat-on-witness-k-prosecution-for-years-despite-advice/10341994>.

195 Ibid.

196 *Criminal Code* (n 7) s 93.1(2).

IV Recommendations for Reform: How Can Academic Freedom Be Protected?

Academic freedom is crucial to the functioning of universities and democratic societies, and central to the production of knowledge and ideas for the public good.[197] The analysis in Part III demonstrates that Australia's espionage offences have the potential to significantly impinge on academic freedom (especially the freedom to teach, discuss, research, disseminate and publish research, engage in intellectual inquiry, contribute to public debate, and even express opinions), yet the framework does not include adequate defences for academics.

In coming to this conclusion, I do not disregard the importance of criminalising espionage. Offences for espionage are a crucial mechanism by which to punish and/or deter those who seek to harm, or gain a benefit over, Australia, including those who seek to do so by stealing valuable research. However, in creating espionage offences, as a nation we must be mindful of how they could apply to scenarios outside genuine espionage, and the consequences of them doing so. The criminalisation of certain research and teaching pursuits creates entire fields that academics are not legally free to pursue, even though such activities may contribute significantly to Australian society. This inherently has the potential to erode academic freedom. While no academic has yet been prosecuted for espionage in Australia,[198] the criminalisation of legitimate research and teaching (and therefore the granting of powers to police to arrest and charge, and to execute search warrants against academics) may certainly be chilling research into criminalised areas. Indeed, it has been argued that 'the mere existence of broad terrorism laws has a chilling effect' on academic freedom.[199] This may have widespread consequences, not just for the higher education and research sector, but also for Australia's democracy and the rule of law.

Therefore, the criminalisation of legitimate research and teaching — especially as a national security offence — is not reasonable or proportionate. The laws criminalise research areas that may be of importance to democratic society, yet penalties have the potential to be severe (depending on the nature of the offending) and the connection between the scope of conduct criminalised and any serious, tangible impact on national security may only be remote. In light of this, it is worth considering whether the espionage provisions could be read down (applying the principle of legality) or invalidated (as incompatible with the implied constitutional freedom of political communication) to protect academic freedom. This discussion will only be brief as these are complicated areas of law and an in-depth consideration of these issues is beyond the scope of this article.

The principle of legality is a common law interpretive technique that broadly operates to determine the legal meaning of statutory provisions by presuming that Parliament does not intend to interfere with fundamental common law rights,

197 See above Part II.

198 There has only been one reported prosecution under Australia's espionage laws since the laws were first introduced in 1914 and that was of a government intelligence analyst: see *R v Lappas* (n 72).

199 Barendt (n 15) 248.

freedoms and principles.[200] The principle can be relevant to statutory interpretation in two ways. First, when the ordinary construction of a provision engages a fundamental common law right (such that it is read down to comply with the right) and/or, second, when there is ambiguity in the statute (such that the ambiguity is resolved in favour of the protection of the right).[201] While the principle of legality was a dominant principle of statutory interpretation under the French High Court,[202] the current Kiefel High Court has tempered the strictness with which it is applied so it may be less likely to assist if the meaning of the espionage laws were to become an issue before the courts.[203]

Furthermore, there may not be sufficient ambiguity in the espionage laws for the principle of legality to become applicable, and there are also real doubts around whether academic freedom amounts to a 'fundamental common law right or freedom'. As yet, there has been no authoritative statement on which common law rights and principles are fundamental,[204] but rather this is something that is 'ultimately a matter of judicial choice'.[205] While the High Court recently gave legal weight to academic freedom (in the case of *Ridd v James Cook University*),[206] there was nothing in that case to suggest that the court considered the freedom to be fundamental. As such, it is unlikely that the courts will be able to use the principle of legality to read down the espionage laws so that they comply with academic freedom.

This contrasts with other freedoms, such as the implied constitutional freedom of political communication (which is derived from the *Australian Constitution*, but is also considered to be a fundamental common law freedom).[207] In constitutional cases, the principle of legality can be applied to determine the meaning of statutes by reading them down to ensure their compliance with constitutional principles.[208] While this could ultimately avoid the need to consider issues of constitutional compliance, it may not be sufficient to secure validity.[209]

There may be times when academic research and teaching (amounting to an espionage offence) falls within the scope of 'political communication',[210] given the espionage offences primarily target national security and international relations information. In such circumstances, there is a possibility that the constitutional

---

200 See, eg, Dan Meagher, 'On the Wane? The Principle of Legality in the High Court of Australia' (2021) 32(1) *Public Law Review* 61, 64 ('On the Wane?'); Bruce Chen, 'The French Court and the Principle of Legality' (2018) 41(2) *Melbourne University Law Review* 401, 401, 404–5 ('The French Court'). See also Bruce Chen, 'The Principle of Legality: Issues of Rationale and Application' (2015) 41(2) *Monash University Law Review* 329 ('The Principle of Legality').

201 Chen, 'The Principle of Legality' (n 200) 340–2.

202 See Chen, 'The French Court' (n 200).

203 See Meagher, 'On the Wane?' (n 200).

204 Chen, 'The Principle of Legality' (n 200) 343–7.

205 Dan Meagher, 'The Common Law Principle of Legality in the Age of Rights' (2011) 35(2) *Melbourne University Law Review* 449, 459.

206 *Ridd v JCU* (n 19). See above Part II.

207 Meagher, 'On the Wane?' (n 200) 62–6, 76–8; Dan Meagher, 'Is There a Common Law "Right" to Freedom of Speech?' (2019) 43(1) *Melbourne University Law Review* 269, 272–3 ('Freedom of Speech').

208 Meagher, 'On the Wane?' (n 200) 63, 77; Chen, 'The French Court' (n 200) 418–22.

209 Ibid.

210 For a discussion of the meaning of 'political communication', see Dan Meagher, 'Freedom of Speech' (n 207) 280–2.

validity of the provisions could be challenged. However, previous cases before the High Court suggest that, in cases involving the implied freedom and national security considerations, national security can act as a trump over the implied freedom (and other constitutional values).[211] It is therefore questionable whether the High Court would in fact strike down the espionage provisions for invalidity (or indeed give them a legal meaning that favours the implied freedom, given it may be difficult to find an interpretation that would distinguish between the conduct of academics and genuine spies). As such, it is uncertain whether a challenge to the espionage laws on the basis of the implied freedom would succeed. Discussion of exactly how the laws could be challenged on this ground is beyond the scope of this article.

Even if the espionage provisions could be invalidated or read down (in accordance with either the implied freedom or academic freedom), to do this would require a relevant case to go to court, which may take a long time (or may never occur). In the meantime, the apparent scope of the laws has the potential to have a significant chilling effect on academic research and teaching, which, in itself, is detrimental to academic freedom. It is clear, therefore, that stronger protections for academics are needed.

What, then, can be done to uphold academic freedom while ensuring Australia's espionage laws still effectively address modern espionage (including espionage against the higher education and research sector, which might be conducted by people who use academic activities as a cover)? I make four recommendations for reform.

First, uncertain key terms used in the espionage framework must be clarified. In particular, greater legislative guidance should be given as to the meaning of 'prejudice' and 'advantage'. This could be achieved, for example, by explaining that prejudice 'includes harm, disadvantage and detriment'. 'Prejudice' and 'advantage' are central to proof of the fault element of certain underlying offences and current definitions mean that it is possible for academics to have satisfied that element. While academics might still satisfy the element with more clearly defined terms, these amendments may exclude academics whose conduct could currently be considered 'prejudicial' but not serious enough to warrant criminalisation (for example, where their research results in criticism of Australian intelligence policies or practices).

Additionally, the definition of 'information' should be amended so that it does not include opinions. Including opinions within the definition of 'information' extends the meaning of the term beyond what is necessary to capture genuine espionage, while also applying to a large proportion of 'information' dealt with by academics (who regularly express their opinions).

Second, sub-offences that criminalise recklessly prejudicing Australia's national security or advantaging the national security of a foreign country should be repealed.[212] Those offences risk criminalising academics who may not have specifically intended certain national security consequences, but who may still have

[211] Rebecca Ananian-Welsh and Nicola McGarrity, 'National Security: A Hegemonic Constitutional Value?' in Rosalind Dixon (ed), *Australian Constitutional Values* (Hart Publishing, 2018) 267, 274–7.

[212] See *Criminal Code* (n 7) ss 91.1(2), 91.2(2), 91.8(2).

been aware of a risk that their work might prejudice or advantage national security (for example, academics who research anything related to defence, intelligence or national security more broadly). Similarly, the Espionage on behalf of a Foreign Principal sub-offence that does not include any fault element in relation to national security should be repealed,[213] being even more far-reaching than the recklessness sub-offence. For example, that offence could apply to academics collaborating with colleagues from foreign universities in countries that are not close allies with Australia on projects broadly related to national security or defence. Repealing this sub-offence and the recklessness sub-offence would be a significant step towards protecting academics who collaborate with colleagues overseas.

Third, the Authorised Prior Publication and Unauthorised Prior Publication defences should be extended to all offences. Currently, neither defence applies to the Solicitation and Preparatory Offences and the Unauthorised Prior Publication defence does not apply to Communication Espionage, the Espionage on behalf of a Foreign Principal offences or the Core Espionage Offence (where the prosecution relies on the fault element of prejudice to Australia's national security). The espionage-related offences pose a significant risk to academics while the latter three offences might still have the capacity to criminalise academics whose research relates to national security (as broadly as it has been defined), even with the above reforms. This is because academics might still fall foul of an 'intention to prejudice Australia's national security or advantage the national security of a foreign country' (for example, where they intend to reveal Australian Government misconduct). The Authorised and Unauthorised Prior Publication defences would provide greater protection for academics by protecting dealings with government-published information and some dealings with non-government sourced information.

Even if these defences were extended, however, there would still be significant gaps in the protection framework. Specifically, academics would not be protected where their research relied on previously unpublished information (such as where they generated their own data through, for example, surveys). Nor would they be protected where they knew that re-publishing the information might prejudice Australia's national security.[214] This might arise where the information was initially published innocuously, or the academic drew together several pieces of less well-known information, and published this in an article with a major journal.

To remedy these gaps, a new defence should be introduced to protect academics engaged in legitimate research and teaching activities. This defence could be adapted from the news reporting defence to Federal secrecy offences.[215] The news reporting defence arises where the person dealt with the information in their 'capacity as a person engaged in the business of reporting news, presenting current affairs or expressing editorial or other content in news media' and at the time they 'reasonably believed that engaging in that conduct was in the public interest' (or they were an administrative staff member acting on behalf of a journalist, editor or

---

213 Ibid s 91.8(3).

214 Ibid ss 91.4(3)(d)–(e).

215 See ibid s 122.5(6). For more on this offence and defence, see James Meehan, 'Protecting Public Interest Journalism in Australia: A Defence to Information Secrecy Offences' (2020) 23(4) *Media and Arts Law Review* 347.

lawyer who believed this).[216] While 'public interest' has not been defined in the *Criminal Code*, the Act provides that the person may not have reasonably believed their conduct was in the public interest if they published the identity of an Australian intelligence agency staff member or witness protection program participant, or where they engaged in the conduct for the purpose of assisting a foreign intelligence agency or military organisation.[217]

This kind of defence could be introduced to protect academics (and their associates) who might have contravened an espionage offence while engaging in legitimate academic activities. To avoid problems with determining who should be included within the defence, it should focus on the academic *activity* rather than the person's role, affiliation, employment or education. This is consistent with Evans and Stone who argue that academic freedom should protect activities that are part of the research and teaching mission of the university and, by extension, anyone who engages in those activities (such as laboratory assistants, librarians, research assistants, PhD candidates and, I would argue, even journal editors, book publishers and conference organisers).[218]

Applying this approach, the 'academic activities' defence should arise where the person deals with the information 'in the course of engaging in academic research and teaching activities'. Unlike the news reporting defence, which has been criticised for excluding journalistic sources as well as certain journalists,[219] this defence would apply to anyone engaged in legitimate academic teaching and research endeavours. Whether something amounts to an 'academic activity' would be for the court to determine.

Some might question whether the defence should extend to other researchers, such as those working for think tanks. Consideration of this issue is, however, beyond the scope of this article (which has focused solely on *academic* freedom). As Evans and Stone highlight, however, academics are distinct from other researchers as they adhere to independently developed research methods, which gives their research 'unrivalled breadth, authority and independence'.[220] This partly justifies why academics are deserving of such a strong freedom and could warrant an academic activities defence that applies only to academics.

To ensure genuine espionage is excluded from operation of the academic activities defence, it would also be necessary to include a limiting element like that included in the news reporting defence.[221] Such an element could specify that it is necessary that 'at the time the person dealt with the information they reasonably believed that engaging in that conduct was in the public interest'. 'Public interest' could be defined in a similar way as the news reporting defence — specifically, that the person may not have reasonably believed that the conduct was in the public

---

216 *Criminal Code* (n 7) s 122.5(6).
217 Ibid s 122.5(7).
218 Evans and Stone (n 16) 56. It has also been argued that this approach should be taken in relation to journalistic activities: see Peter Greste, *Define Journalism; Not Journalists* (Press Freedom Policy Papers Reform Briefing 3/2021, 2021).
219 See Meehan (n 215); Ananian-Welsh, Kendall and Murray (n 9) 810.
220 Evans and Stone (n 16) 51.
221 See *Criminal Code* (n 7) s 122.5(6)(a).

interest if they engaged in the conduct for the purpose of assisting a foreign intelligence agency or military organisation.[222] In this way, the defence would not be available to people who use academic activities as a cover to engage in espionage. Such a defence would go a long way towards ensuring that Australia's espionage laws still capture espionage against the higher education and research sector, while providing a mechanism to protect legitimate academic research and teaching activities more effectively.

V Conclusion

In this article I assessed the impact of Australia's espionage laws on legitimate academic research and teaching pursuits and, consequently, on academic freedom. My analysis showed that five of Australia's espionage offences pose a very real threat to academics. These offences are the Core Espionage Offence, Communication Espionage, the Preparatory Offence and, for academics collaborating with or employed by foreign public universities or research organisations, Espionage on behalf of a Foreign Principal offences and the Solicitation Offence.

The offences pose a risk to academics whose research and teaching involves in any way defence, military, intelligence, national security or international relations information (especially if it critiques Australia or could benefit the national security of another country), regardless of how that research is conducted. This means that the laws could apply to academics in the fields of political science, international relations, peace and conflict studies, law, criminology, history, geography and STEM, among others. Furthermore, because the offences are concerned with dealings with information, they could apply to any part of the research and teaching process, from preliminary research and communications with colleagues to publications, presenting research at conferences, and teaching students in class.

As such, the espionage laws have the potential to criminalise the work of certain academics — without the protection of adequate defences. This may lead to the chilling of research into areas that may benefit Australian society and democracy. In doing so, these national security laws may indeed threaten academic freedom. To ensure this freedom is upheld, I recommend several reforms be made. Significantly, these include a defence for legitimate academic research and teaching activities. Such a defence would be a significant step towards ensuring academic freedom is better protected in Australia, while allowing for the prosecution of genuine espionage.

[222] See ibid s 122.5(7)(d).