*Brendan Walker-Munro**

RISKS OF ESPIONAGE IN OUR UNIVERSITIES? LESSONS ON RESEARCH SECURITY FROM *LI V CANADA*

Abstract

In the 2023 case of *Li v Canada*, the Canadian Federal Court upheld the refusal of a visa for Chinese national, Yuekang Li, based on his apprehended risk of engaging in espionage. Yet this decision is only the latest in a string of cases in Canada evidencing a tougher stance on research security — that is, the protection of certain university research and programs with national security dimensions. In Australia, where research security is almost entirely absent from political and policy discourse, what is the potential role of migration law in the pursuit of research security? Can Australia learn anything from Canada's experience? The answers to these questions help inform not only Australia's burgeoning migration law scholarship, but also future pathways for the due recognition of research security in this country.

I Introduction

In the late 2023 decision of *Li v Canada* ('*Li*'),[1] the Canadian Federal Court ('CFC') affirmed the refusal of a student visa to a prospective international PhD student, Mr Yuekang Li. Ordinarily, this would not make the national headlines — except in this case, the PhD student was a Chinese national and the refusal was on the basis of an apprehended risk of Mr Li being 'targeted and coerced into providing information that would be detrimental to Canada or contrary to Canada's interests'.[2] The case immediately drew media attention, with some labelling the decision 'deeply unhelpful',[3] an unacceptable example of 'pre-crime',[4] and a strong disincentive for

* Senior Lecturer, Faculty of Business, Law and Arts, Southern Cross University.

1 [2023] FC 1753 ('*Li*').

2 Ibid [17], [63].

3 Alex Usher, 'A Deeply Unhelpful Federal Court Ruling', *Higher Education Strategy Associates* (Blog Post, 10 January 2024) <https://higheredstrategy.com/a-deeply-unhelpful-federal-court-ruling/>.

4 Creso Sá, 'A "Precrime" Has Been Prevented — Or Has It?', *University Affairs* (Blog Post, 12 January 2024) <https://www.universityaffairs.ca/opinion/policy-and-practice/a-precrime-has-been-prevented-or-has-it/>.

international students to attend Canadian universities (which may have been the CFC's intention).[5]

Universities are having to contend with just these types of geopolitical challenges on an unprecedented scale, where the *domaine réservé* of national security sits uncomfortably beside notions of open science and academic inquiry. Previously funded by incredibly high engagement with international student cohorts and research arrangements with international entities,[6] universities are now being forced to question the closeness of these associations.[7] Universities are now seen as prime targets for physical or 'in-person' espionage,[8] as well as virtual or cyberespionage (a domain where universities have long struggled to protect themselves).[9] In response, governments and institutions have taken a variety of approaches across the law and policy

5 CBC, 'Court Decision Barring Chinese Student Sends Message About Espionage Risk, Experts Say', *Yahoo! News Canada* (online, 5 January 2024) <https://ca.news.yahoo.com/court-decision-barring-chinese-student-225416110.html>.

6 See, eg, Joint Standing Committee on Foreign Affairs, Defence and Trade, Parliament of Australia, *Inquiry into Australia's Tourism and International Education Sectors* (Interim Report, October 2023) 12–13, 33–4.

7 Radomir Tylecote and Robert Clark, *Inadvertently Arming China? The Chinese Military Complex and its Potential Exploitation of Scientific Research at UK Universities* (Final Report, Civitas, February 2021); Brendan Walker-Munro, Ruby Ioannou and David Mount, *Are We Training Potential Adversaries? Australian Universities and National Security Challenges to Education* (Final Report, 30 October 2023).

8 See, eg: Ana Swanson and Keith Bradsher, 'White House Considers Restricting Chinese Researchers Over Espionage Fears', *New York Times* (online, 30 April 2018) <https://www.nytimes.com/2018/04/30/us/politics/trump-china-researchers-espionage.html>; Erin N Grubbs, 'Academic Espionage: Striking the Balance Between Open and Collaborative Universities and Protecting National Security' (2019) 20(5) *North Carolina Journal of Law and Technology* 235; Ken Dilanian, 'American Universities Are a Soft Target for China's Spies, Say US Intelligence Officials', *NBC News* (online, 3 February 2020) <https://www.nbcnews.com/news/china/american-universities-are-soft-target-china-s-spies-say-u-n1104291>; Louise Ayling, 'How a Major Spy Ring is Operating on Australian Soil and "Conducting Clandestine Intelligence Collection", Harassing Expatriates and Sending Information to Other Countries', *Daily Mail* (online, 25 February 2020) <https://www.dailymail.co.uk/news/article-8038051/Major-spy-ring-Australia-clandestine-intelligence-collection-harassing-expatriates-foreign-agents.html>; Gordon Corera, 'Iranian Hackers Posed as British-based Academic', *BBC News* (online, 13 July 2021) <https://www.bbc.com/news/technology-57817463>.

9 See, eg: Ivano Bongiovanni, 'The Least Secure Places in the Universe? A Systematic Literature Review on Information Security Management in Higher Education' (2019) 86 *Computers and Security* 350; Peter Romness, 'Securing University Research: An Industry Perspective', *Cisco Blogs* (Blog Post, 13 April 2021) <https://blogs.cisco.com/education/securing-university-research-an-industry-perspective>; Jin Li, Wei Xiao and Chong Zhang, 'Data Security Crisis in Universities: Identification of Key Factors Affecting Data Breach Incidents' (2023) 10 *Humanities and Social Sciences Communications* 1.

spectrum, from centralisation of policy and the broadening of export controls,[10] to recommendations that funding bodies impose research security obligations through grant contracts.[11]

The implications of some types of research security programs on universities have been tremendous. The United States' 'China Initiative' — a program by the Department of Justice and the Federal Bureau Investigation to surveil Chinese academics for risks of espionage — was abandoned after failed prosecutions and allegations of racial bias.[12] Imposing national security rules on a profession that embraces publication and open collaboration harms academic freedom and chills intellectual inquiry.[13] There is also a suggestion in the literature that research security programs that are hastily or arbitrarily imposed could compromise international legal obligations, such as a 'right to science', which may arguably be derived from the *International Covenant on Economic, Social and Cultural Rights*.[14]

The decision in *Li* also forms part of this broader web of actions by Canada to enhance research security. The Canadian government defines research security as 'the ability to identify possible risks to your work through unwanted access, interference, or theft and the measures that minimize these risks and protect the inputs, processes, and products that are part of scientific research and discovery'.[15] In 2020, the Canadian government launched a centralised research security portal, and subsequently issued the *National Security Guidelines for Research Partnerships* ('Canadian Guidelines') on 12 July 2021.[16] The Canadian Guidelines mandated that recipients of federal funding conduct risk assessments on both the nature of research

10 Alex Wilner et al, 'Research at Risk: Global Challenges, International Perspectives, and Canadian Solutions' (2022) 77(1) *International Journal* 26; Caroline Winter, 'Research Security and Open Scholarship in Canada', *Open Scholarship Policy Observatory* (Web Page, 17 November 2023) <https://ospolicyobservatory.uvic.ca/research-security-and-os-in-canada/>.

11 Tommy Shih, 'The Role of Research Funders in Providing Directions for Managing Responsible Internationalization and Research Security' (2024) 201(1) *Technological Forecasting and Social Change* 123253.

12 Margaret K Lewis, 'Dismounting the "China Initiative" Tiger' (2021) 52 *Seton Hall Law Review* 987.

13 Grubbs (n 8); Ot van Daalen, 'In Defense of Offense: Information Security Research Under the Right to Science' (2022) 46 *Computer Law and Security Review* 105706.

14 Brendan Walker-Munro, *A Duty to Protect from Science? Interactions in International Law Between Research Security and the Right to Science* (Report, 23 May 2024); *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(1)(b).

15 'Why Safeguard Your Research?', *Government of Canada* (Web Page, 5 May 2022) <https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/why-safeguard-your-research> ('Why Safeguard Your Research?').

16 Innovation, Science and Economic Development Canada, *National Security Guidelines for Research Partnerships* (January 2024).

being conducted and the entities with whom the research was being conducted.[17] The purpose of the Canadian Guidelines was to:

> … help safeguard Canada's research ecosystem from foreign interference, espionage, and unwanted knowledge transfer that could contribute to: advancements in military, security, and intelligence capabilities of states or groups that pose a threat to Canada; or disruption of the Canadian economy, society, and critical infrastructure.[18]

Following the issue of the Canadian Guidelines, two separate joint statements by the Canadian Minister of Innovation, Science and Industry, Minister of Health, and Minister of Public Safety have made clear that research security is a top priority of the Canadian government and would be pursued through robust application of both law and policy.[19]

Australia has no such unified government agenda on research security. Although the Australian government, through the Universities Foreign Interference Taskforce ('UFIT'), published *Guidelines to Counter Foreign Interference in the Australian University Sector* ('UFIT Guidelines') in 2019 (and later refreshed them in 2021),[20] the UFIT Guidelines are voluntary. They are not universally applied by all Australian universities in the same way,[21] and are not mandated requirements for seeking federal funding from the Australian Research Council ('ARC'). Nor does the Australian government have a federally articulated research security policy. Despite an inquiry by the Parliamentary Joint Committee on Intelligence and Security making 27 recommendations in March 2022,[22] almost none of those recommendations have been successfully implemented, and some were outright rejected by the Commonwealth Government.[23] In December 2023, the ARC published a Countering Foreign Interference Framework;[24] however, this does not analyse the full scope of risks

---

17 Ibid 9–11.

18 Ibid 4.

19 Innovation, Science and Economic Development Canada, 'Statement from Minister Champagne, Minister Duclos and Minister Mendicino on Protecting Canada's Research' (Press Statement, 14 February 2023); Innovation, Science and Economic Development Canada, 'Statement from Minister Champagne, Minister Holland and Minister LeBlanc on New Measures to Protect Canadian Research' (Press Statement, 16 January 2024).

20 University Foreign Interference Taskforce, *Guidelines to Counter Foreign Interference in the Australian University Sector* (Department of Education, Skills and Employment, 17 November 2021).

21 Department of Education, *Report on Implementation of the Guidelines to Counter Foreign Interference in the Australian University Sector* (Report, August 2023).

22 Parliamentary Joint Committee on Intelligence and Security, *Inquiry into National Security Risks Affecting the Australian Higher Education and Research Sector* (Final Report, March 2022) [6.8]–[6.120].

23 Department of Home Affairs, *Australian Government Response to the Parliamentary Joint Committee on Intelligence and Security Report: National Security Risks Affecting the Australian Higher Education and Research Sector* (Report, February 2023).

24 Australian Research Council, 'ARC Countering Foreign Interference Framework' (December 2023).

associated with research security and is limited to a small subset of due diligence checks able to be conducted on publicly sourced information.[25] An important note is that each of these policy tools have not focused on the broader notion of research security, but on foreign interference — merely one of the many risks facing our higher education sector.

This article will therefore consider whether the use of migration law as a tool for research security in Australia is appropriate, given its reliance on Ministerial executive power and discretion, often applied in a manner detrimental to the applicant where issues of national security are invoked. Part II of this article will present the case of *Li*, including the originating decision but with specific focus on the CFC's novel interpretation of the term 'espionage' in the context of Canada's recent moves to tighten their research security frameworks. Part III will then conduct a brief examination of Canadian migration law and research security policy to demonstrate why *Li* is so important to the use of migration law as a research security control.[26] Part IV will then present the equivalent Australian provisions that might be relied upon in an Australian case touching upon research security. Part V then examines the tensions or limits of using migration law as a mechanism for protecting research security, rather than relying primarily on other areas of law such as criminal law or sanctions law, or domestic regulation of universities as statutory creatures. Part VI will conclude with some recommendations for policy development and future research in this critical area. In its approach, this article has two aims. The first is to contribute to the overall discourse regarding how migration law has served the Executive — particularly the Minister for Immigration and Multicultural Affairs — in achieving their policy objectives, which increasingly refer to notions related to research security. The second is to bring attention to the Canadian legal framework, case law (following the *Li* decision), and academic analysis as a comparative jurisdiction that has considered similar conceptual questions and may therefore have instructive lessons for Australia.

II The Facts and Decision in *Li*

Yuekang Li was a resident and citizen of the People's Republic of China ('PRC') admitted to the PhD program of the University of Waterloo in Canada in April 2022.[27] As part of his studies, Mr Li applied in September 2022 for a study permit under Canada's *Immigration and Refugee Protection Act* ('*IRPA*')[28] and *Immigration and Refugee Protection Regulations* ('*IRPR*').[29] The issue of a Study Permit requires a security assessment of the prospective applicant,[30] meaning the processing of the application

25 Ibid 6; Brendan Walker-Munro, '(Professor) Hadrian's Wall: The Role of the Australian Research Council in Securing University Research' (2024) *UNSW Law Journal*, forthcoming.

26 For the United States example, see Alex Nowrasteh, *Espionage, Espionage-Related Crimes, and Immigration* (Report No 909, 9 February 2021).

27 *Li* (n 1) [6].

28 Ibid; *Immigration and Refugee Protection Act*, SC 2001, c 27 ('*IRPA*').

29 *Immigration and Refugee Protection Regulations*, SOR/2002–227 ('*IRPR*').

30 Ibid s 216(1).

was quite protracted.[31] When Mr Li sought judicial review of that delay, it became clear in tendered documents that Mr Li's permit had been recommended for refusal, as there were 'reasonable grounds to believe that he is inadmissible to Canada'.[32]

The security grounds provision in the *IRPA*, s 34(1), deems a person to be inadmissible to Canada if there 'are reasonable grounds to believe that any of the following have occurred, are occurring or may occur' in relation to that person:

> (a) engaging in an act of espionage that is against Canada or that is contrary to Canada's interests;
> (b) engaging in or instigating the subversion by force of any government;
> (b.1) engaging in an act of subversion against a democratic government, institution or process as they are understood in Canada;
> (c) engaging in terrorism;
> (d) being a danger to the security of Canada;
> (e) engaging in acts of violence that would or might endanger the lives or safety of persons in Canada; or
> (f) being a member of an organization that there are reasonable grounds to believe engages, has engaged or will engage in acts referred to in paragraph (a), (b), (b.1) or (c).

The specific nature of the concerns were outlined in the decision by the Minister's delegate as being a combination of 'Mr Li's education, his field of study and research in Canada, and open-source information reporting on the PRC's reliance on non-traditional collectors of information, including science and technology students, to advance China's military and other interests'.[33] It was this combination of factors which presented a risk of Mr Li 'engaging in an act of espionage that is against Canada or that is contrary to Canada's interests'.[34] The Chief Justice noted that no Act of the Canadian Parliament had defined the word 'espionage', but at its most basic it constituted 'the secret, clandestine, surreptitious or covert gathering or reporting of information to a foreign state or other foreign entity or person', where 'such activity is against Canada or is contrary to Canada's interests'.[35] That conclusion was reinforced by the CFC's previous decisions in: (1) *Crenna v Canada* ('*Crenna*'),[36] where the CFC held that espionage involved 'gathering' information that was conducted secretly, covertly, or clandestinely; and (2) *Qu v Canada* ('*Qu*')[37] and *Peer v Canada* ('*Peer*'),[38] where the CFC held that espionage included reporting

---

31 *Li* (n 1) [8].

32 Ibid [9]–[11]; *IRPA* (n 28) ss 34(1)(a), 87, 83(1)(d).

33 *Li* (n 1) [14].

34 *Li* (n 1) [77]; *IRPA* (n 28) s 34(1)(a).

35 *Li* (n 1) [32] (emphasis omitted).

36 [2020] FC 491 ('*Crenna*').

37 [2000] 4 FC 71 ('*Qu*'). See also *Qu v Canada (Minister of Citizenship and Immigration*) [2002] 3 FC 3. Though *Qu* was a decision prior to the enactment of the *IRPA* (n 28), Crampton CJ observed that 'the pre-IRPA jurisprudence with respect to the meaning of "espionage" continues to be good law': *Li* (n 1) [45], citing *Sumaida v Canada (Citizenship and Immigration)* [2018] FC 256, [21] ('*Sumaida*').

38 [2010] FCA 752 ('*Peer*').

information conducted secretly, covertly, or clandestinely.[39] Further, CFC confirmed in 2022 that the impugned activity did not need a nexus to the commonly understood concept of 'national security'.[40]

His Honour then referred specifically to 'open-source' (ie, publicly available) information which stated 'the PRC relies on non-traditional collectors of information to target non-governmental organizations in Canada, including academic institutions and businesses'.[41] The loss or unauthorised disclosure of such information to such 'non-traditional collectors' could conceivably 'have a negative impact on the safety, security or prosperity of Canada' and thus be 'contrary to Canada's interests'.[42] With regard to Mr Li's chosen field of study — indicated as microfluidics — his Honour noted that the open-source material relied upon by the Minister's delegate included references to the PRC naming microfluidics as a growth industry as well as contributing to their 'top ten' targeted high-tech industries (advanced medical products).[43]

What is perhaps the most novel aspect of *Li* is the CFC's validation of the decision-maker's finding that the espionage criterion could be fulfilled by an applicant being 'targeted and coerced into providing information that would be detrimental to Canada or contrary to Canada's interests'.[44] Such targeting and coercion may occur, it would seem, independent of the applicant's intentions and consent, and at any time before, during or after their time in Canada.[45]

Immediately after Mr Li's case, another PhD student — this time an Iranian computer engineer — was refused a visa for purportedly 'being a danger to the security of Canada'.[46] A week later, the Canadian government published strict new guidelines which prohibited research collaborations with hundreds of named entities in China, Russia and Iran.[47] Thus, Mr Li's decision addresses significant issues for Canada,

39 Ibid [28], [35].

40 See, eg, *Canada (Citizenship and Immigration) v Mason* [2022] 1 FCR 3 ('*Mason*').

41 *Li* (n 1) [52].

42 Ibid [68].

43 Ibid [54]–[56].

44 Ibid [17], [63]. It is to be emphasised that it was the immigration officer's decision that held this could be captured by s 34(1)(a) of the *IRPA* (n 28). The CFC merely upheld that such a decision was not unreasonable.

45 *Li* (n 1) [65]–[66].

46 Jim Bronskill, 'Iranian Student, Denied Permit to Study in Canada, Disputes Security Danger Label', *CityNews* (online, 9 January 2024) <https://kitchener.citynews.ca/2024/01/09/iranian-student-denied-permit-to-study-in-canada-disputes-security-danger-label/>.

47 Omair Quadri, 'Ottawa Clamps Down on University Research Partnerships with China, Iran and Russia', *The Globe and Mail* (online, 17 January 2024) <https://www.theglobeandmail.com/canada/article-morning-update-ottawa-clamps-down-on-university-research-partnerships/>; Government of Canada, *Named Research Organizations* (Policy Document, January 2024) ('*Named Research Organizations*').

which aims to become a world leader in research security, including identifying risks to research and taking action to 'protect the inputs, processes, and products that are part of scientific research and discovery'.[48] The use of immigration law to protect Canadian research security interests can hardly be seen as surprising — espionage from inside a country is far easier than from outside it. But is migration law an ideal tool for providing research security? What tensions does it create with the notions of academic freedom and open intellectual inquiry which university research seeks to uphold? In the next Part, I will examine the Canadian research security framework and how some of the migration law provisions could apply in that context.

III Canadian Migration Law and Research Security

Canada has had a reasonably swift introduction to the practice of research security. The federal government first published a research security policy position in 2021, which asked the Government-Universities Working Group to 'develop specific risk guidelines to integrate national security considerations into the evaluation and funding of research partnerships'.[49] The subsequent 'Safeguarding Research' portal defined research security as the 'ability to identify possible risks to your work through unwanted access, interference, or theft and the measures that minimize these risks and protect the inputs, processes, and products that are part of scientific research and discovery'.[50] More recently, Canada has been spurred by recent scandals in research[51] to engage in crackdowns in academic contexts through a tripartite national policy response: the *Policy on Sensitive Technology Research and Affiliations of Concern*,[52] the list of *Sensitive Technology Research Areas*,[53] and the *Named Research Organisations* ('NRO') identifying entities which could pose a risk to Canada's national security.[54]

The *IRPA* has a clear role to play in securing Canadian national security in general, and research security in particular. This is because s 34(1) of the *IRPA* renders inadmissible to Canada any person who poses a risk of espionage, subversion of

48 Why Safeguard Your Research? (n 15).

49 Innovation, Science and Economic Development Canada, 'Research Security Policy Statement — Spring 2021' (Press Statement, 24 March 2021).

50 Why Safeguard Your Research? (n 15).

51 See, eg: Bob Young, 'Foreign Interference / Influence in Canada: A Way Forward' (2023) 6(2) *Journal of Intelligence, Conflict, and Warfare* 79; Brendan Walker-Munro, 'Canada's Biosecurity Scandal: The Risks of Foreign Interference in Life Sciences', *The Strategist* (online, 2 April 2024) <https://www.aspistrategist.org.au/canadas-biosecurity-scandal-the-risks-of-foreign-interference-in-life-sciences/>.

52 Government of Canada, *Policy on Sensitive Technology Research and Affiliations of Concern* (Policy Document, January 2024).

53 Government of Canada, *Sensitive Technology Research Areas* (Policy Document, January 2024).

54 *Named Research Organizations* (n 47).

the government, acts of terrorism or violence, or otherwise 'being a danger to the security of Canada'. Section 34 in the *IRPA* was amended on 19 June 2013 by the *Faster Removal of Foreign Criminals Act* ('*Faster Removal Act*'),[55] which changed s 34(1)(a) from 'engaging in an act of espionage or an act of subversion against a democratic government, institution or process as they are understood in Canada' to the current form of 'engaging in an act of espionage that is against Canada or that is contrary to Canada's interests'.[56] This amendment was intended to provide an exclusion for 'those who may have been involved in espionage for close democratic allies of Canada and who may in fact have been gathering intelligence on behalf of Canada against common security threats'.[57] As an unintended benefit, it dealt with a potential loophole in the *IRPA* which prevented inadmissibility decisions being made against persons who committed espionage against States that were not democracies at the time of their conduct.[58] That definition of espionage, contrary to s 34(1)(a) of the *IRPA*, remained largely undisturbed for a number of years, and appeared routinely in declarations of inadmissibility to Canada for former employees of the intelligence services of Iran,[59] Ethiopia,[60] Sudan[61] and Syria.[62]

One of the earliest cases of applying the espionage provision of the *IRPA* arose in the 2003 case of *Gariev v Canada*.[63] Viatcheslav Gariev was a Belarusian citizen who served in the armed forces of the former Soviet Union as a computer programmer

55 *Faster Removal of Foreign Criminals Act*, SC 2013, c 16.

56 Ibid s 13(2).

57 Canada, *Parliamentary Debates*, House of Commons, 24 September 2012, 10327 (Jason Kenney).

58 *X v Canada (Public Safety and Emergency Preparedness)* [2009] CanLII 49233.

59 One case succeeded at judicial review because the original decision relied on s 34(1)(d) of the *IRPA* and declared the applicant a 'danger to Canada' without requisite evidence: *Hosseini v Canada (Immigration, Refugees and Citizenship)* [2018] FC 171. The second case was uncontroversial because the applicant had published his autobiography in which he laid out his extensive intelligence work: *Sumaida* (n 37) [1].

60 *X (Re)* [2019] CanLII 142993 ('*X (Re)* 142993'); *X (Re)* [2019] CanLII 132626 ('*X (Re)* 132626'); and *X (Re)* [2019] CanLII 135483 ('*X (Re)* 135483') are three such decisions involving inadmissibility to Canada of former employees of the Ethiopian Information Network Security Agency ('INSA'), which conducted spying on dissidents, journalists, and Ethiopian expatriates. Cf *Gaga v Canada (Citizenship and Immigration)* [2020] FC 607 where the CFC allowed judicial review despite evidence of employment of the Applicant by INSA because the Immigration Division merely adopted the reasons of another decision-maker 'without showing clear engagement with the issues [so] does not meet the requirements of justification, transparency and intelligibility': at [22], citing *Dunsmuir v New Brunswick* [2008] 1 SCR 190; *Canada (Minister of Citizenship and Immigration) v Vavilov* [2019] SCC 65.

61 *X (Re)* [2020] CanLII 125445 ('*X (Re)* 125445'), which was upheld on review: *Ibrahim v Canada (Citizenship and Immigration)* [2022] FC 1299.

62 *Al Ayoubi v Canada (Citizenship and Immigration)* [2022] FC 385.

63 [2004] FC 531.

and worked on 'intercepting and deciphering communications from Europe'.[64] Mr Gariev was deemed inadmissible under s 34(1)(f) of the *IRPA*, because his previous service with Russian military intelligence (now commonly known by the abbreviation 'GRU') constituted membership 'of an organization that there are reasonable grounds to believe engages, has engaged, or will engage in acts [of espionage]'.[65] Similar conclusions were reached in *Canada v Abramishvili*,[66] *Lennikov v Canada*,[67] *Moiseev v Canada*,[68] and *Zhulanov v Canada*[69] where members of the former Soviet KGB were held to be inadmissible under s 34(1)(f) because of that membership.[70] Thus in the research security context, membership of any type of organisation with security implications would be sufficient ground for an inadmissibility decision.

Two cases then established the groundwork for judicial interpretation of the espionage provision in the *IRPA*: *Peer* and *Afanasyev.* In *Peer*,[71] a Pakistani citizen (and husband to a Canadian citizen) was found to be inadmissible to Canada because of the espionage provision in the *IRPA* for serving in Pakistan's Corps of Military Intelligence and its Inter-Services Intelligence Directorate.[72] Mr Peer argued his service did not constitute espionage, given his duties were largely equivalent to those of the Canadian Security Intelligence Service ('CSIS') and authorised by Pakistan's domestic law.[73] However, this contention failed because espionage 'does not have to have an illicit outcome as its goal',[74] nor is it 'dependant on whether the person who is engaged in the espionage does so only within the boundaries of his home country and reports to agencies in his home country, as in this case, or does so in a foreign country and reports to agencies of his home country'.[75]

64 Ibid [39].

65 Ibid [2], [37], [41].

66 [2007] CanLII 12841.

67 [2007] FC 43.

68 [2008] FC 88.

69 [2009] CanLII 93270.

70 Since those decisions, other decisions have also determined that it is not necessary for the acts of espionage by an organisation coincide with the timing of membership of the individual in that organisation: *Al Yamani v Canada (Minister of Citizenship and Immigration)* [2006] FC 1457; *Gebreab v Canada (Minister of Citizenship and Immigration)* [2009] FC 1213; *Gebreab v Canada (Minister of Citizenship and Immigration)* [2010] FCA 274.

71 *Peer* (n 38).

72 Ibid [25].

73 Ibid [23], [25]–[26].

74 Ibid [34].

75 Ibid [35]. Affirmed on appeal in *Peer v Canada (Citizenship and Immigration)* [2011] FCA 91.

Afanasyev v Canada[76] involved a decision to refuse Dmytro Afanasyev permanent residence in Canada based on the risk of espionage. Mr Afanasyev was a Ukrainian citizen who served in the Soviet Army from 1985 to 1987 in military signals intelligence, where (according to the CSIS) he was trained in radio intelligence and telecommunications interception.[77] However, Mr Afanasyev described his role as more clerical in nature, involving writing encrypted English words in a report and filing them with a duty officer.[78] In the first case in 2010, the judicial review application succeeded because the Court held that the immigration officer had failed to explain his reliance on CSIS reports over Mr Afanasyev's account of his actions: '[i]n those circumstances, it was imperative for the Officer to explain why he rejected the applicant's explanations'.[79] The Court also held that the immigration officer had failed to articulate how Mr Afanasyev's activities constituted 'espionage' within the meaning of the *IRPA*.[80]

Another case considering the risk of espionage under s 34(1)(a) of the *IRPA* was *Crenna*, where it was alleged that Elena Crenna had cooperated with an agent from the Russian Federal Security Service, who was investigating a construction project at which Ms Crenna worked.[81] The CFC held that Ms Crenna's actions did not engage the espionage definition because they were 'neither secret, clandestine, surreptitious nor covert', and so lacked the requisite character to be considered espionage.[82] *Crenna* thus became an important touchstone because it imported an element of secrecy or covertness that was otherwise lacking in the statutory text into the 'ordinary meaning' of espionage under s 34(1)(a).[83]

Given the global attention on Chinese acts of interference and influence in Canada from 2019 onwards,[84] the notion that espionage could be conducted by non-traditional actors, in non-traditional ways, has started to emerge with repercussions

76 [2010] FC 737 ('*Afanasyev*'). See also *Afanasyev v Canada (Citizenship and Immigration)* [2012] FC 1270.

77 *Afanasyev* (n 76) [4].

78 Ibid [32].

79 Ibid [33]. See also *Okomaniuk v Canada (Citizenship and Immigration)* [2013] FC 473, [25]–[28].

80 *Afanasyev* (n 76) [34], [36].

81 *Crenna* (n 36) [23]–[27].

82 Ibid [59].

83 *X (Re)* 125445 (n 61) [13], [45]; *Gao v Canada* [2022] FC 64, [38]–[39] ('*Gao*').

84 See, eg: Alex Joske, Australian Strategic Policy Institute, *China Defence Universities Tracker* (Report No 23, 25 November 2019); Alex Joske, Australian Strategic Policy Institute, *Hunting the Phoenix* (Report No 35, 20 August 2020); Scott Livingston, Centre for Strategic and International Studies, *The Chinese Communist Party Targets the Private Sector* (Report, 8 October 2020); Jude Blanchette, Centre for Strategic and International Studies, *Strengthening the CCP's "Ideological Work"* (Report, 13 August 2020); Tylecote and Clark (n 7).

for research security. In *Gao v Canada*,[85] the applicant had been employed with the Overseas Chinese Affairs Office ('OCAO') for 20 years and been deemed inadmissible to Canada. The CFC heard evidence that the OCAO was '(i) … involved in covert action *vis-a-vis* overseas Chinese communities, including monitoring their activities and exercising political influence; and (ii) [maintaining] policies on topics including "how to gain and consolidate trust amongst targets, how to actively manage targets and how to supervise their behaviour"'.[86] The CFC held it to be common ground between the parties that

> the OCAO infiltrates the inner workings of the overseas Chinese communities, selectively imparts to them only what they need to know, and denies them access to information that may affect the success of the OCAO and the Communist Party of China's *qiaowu* work. Based on the record, it was reasonable for the Officer to conclude that, in fact, there are reasonable grounds to believe that OCAO engages in covert and surreptitious intelligence gathering.[87]

Following the decision in *Gao*, in *X (Re)*[88] the Immigration Review Board considered the case of a Chinese national who was employed at the Information Engineering University ('PLAIEU') of the People's Liberation Army ('PLA') and purportedly held a military rank. The Board held that '[b]road meaning is to be given to the term "espionage", which has been defined as a method of information gathering, by spying, by acting in a covert way, or through "surreptitious or covert information gathering"'.[89] Applying that definition, the Chinese national was ruled not inadmissible to Canada, as the Minister failed to prove any requisite connection between PLAIEU and bodies of the Chinese state which conducted espionage activities.[90] A later decision of the CFC in *Geng v Canada*[91] — where the applicant was a professor who taught linguistics at the Luoyang Foreign Languages Institutes, including to current and future intelligence operatives of the PLA — held that '[w]hile membership is an expansive concept in the context of *IRPA* s 34, it can't be stretched infinitely'. So, whilst membership can be considered under s 34(1)(f), mere membership of a group is insufficient to find that an applicant is *per se* at risk of engaging in espionage under s 34(1)(a).[92]

---

85 *Gao* (n 83). See also *Zhang v Canada (Public Safety and Emergency Preparedness),* [2023] CanLII 123767.

86 *Gao* (n 83) [33].

87 Ibid [39].

88 *X (Re)* [2021] CanLII 151780.

89 Ibid [26], citing *Qu* (n 37) [12], [33] and *Sumaida* (n 37) [21].

90 Ibid [28]–[32], [73]–[81]. Much of these reasons are redacted, somewhat limiting their utility; cf *Meng v Canada (Public Safety and Emergency Preparedness)* [2023] CanLII 76330, [7], [53]–[57].

91 *Geng v Canada (Citizenship and Immigration)* [2023] FC 773.

92 Ibid [75].

Taking the above cases together, the implications for migration control in research security are relatively straightforward. As early as 2000, the CFC had established that simply 'reporting' information of intelligence value could constitute espionage if it met a 'secret, clandestine, surreptitious or covert' criterion,[93] and this could include publicly available information.[94] That definition of espionage was upheld in *Peer*[95] and not disturbed by the Federal Court of Appeal.[96] From 2013 when the changes in the *Faster Removal Act* took effect, the bar was lowered further to involve conduct either 'against Canada' or 'contrary to Canada's interests'.[97] On that basis, the reporting of 'sensitive' information (but not necessarily information regarding 'national security')[98] contrary to Canada's interests would be espionage.[99] Therefore, where a student, researcher or professor engages in research with 'intelligence value' — whether that research is publicly available or not — and shares that information with a foreign power in a secret, clandestine or surreptitious way, they are likely to be engaging in espionage.

So, what does the *Li* case offer from the perspective of research security? His Honour Crampton CJ held that an individual did not need to be operating under the control or direction of a foreign entity to be at risk of committing espionage contrary to Canada's interests. That position seems broadly analogous to the decision in *Qu*, where the CFC held that '[t]he words "espionage", "sabotage" and "subversive activity" would appear to have no special legal meaning, and they must therefore be given their ordinary meaning … espionage is simply a method of information gathering by spying, by acting in a covert way'.[100]

However interesting, it is entirely possible that the decision in *Li* could have been supplanted by the Federal government policy enacted by Canada shortly after *Li* was decided. Effectively, any researcher (foreign or domestic) now intending to work in a listed sensitive technology research area must not collaborate with any entity on the NRO list and must cease any association before commencing work. Microfluidics would find several bases for inclusion in a sensitive technology research area (under either 'advanced manufacturing' or 'advanced medical/health care'), and Beihang University (where Mr Li completed a bachelor's degree in Mechanical Engineering) is listed on the NRO and has strong ties to the defense industry in the PRC. Therefore, it is unlikely that Mr Li would have been permitted to perform

93 *Qu* (n 37) [45]–[46]; cf *Crenna* (n 36).

94 *Peer* (n 38) [25].

95 Ibid.

96 Ibid.

97 *Weldemariam v Canada (Public Safety and Emergency Preparedness)* [2020] 4 FCR 354, [42].

98 *Mason* (n 40).

99 For example, the reporting on the activities of students: *Qu* (n 34), dissidents: *X (Re)* 142993 (n 60); *X (Re)*132626 (n 60); and *X (Re)* 135483 (n 60), or Chinese nationals: *Gao* (n 78).

100 *Qu* (n 37) [25], [48], quoting *Re Wenberg* (1968) 4 IAC 292, 307.

his research or qualified for the issue of a visa in the first place.[101] Similarly, future researchers — whether students or not — will need to satisfy their *alma mater* that they have no association with any NRO to participate in research in sensitive technology areas, well in advance of any migration process under Canadian law.

I will now turn to Australia — which has no such, or similar, policy — to examine how migration law could enforce research security, and the analogies with Canada's previous approaches.

IV Australian Migration Law and Research Security

Entry to Australia (including for study purposes) for non-citizens (both students and academics) is regulated by the *Migration Act 1958* (Cth) ('*Migration Act*') and the *Migration Regulations 1994* (Cth).[102] To qualify for a visa, applicants must satisfy a number of statutory criteria — for this article I will limit the consideration of these to the public interest criteria ('PIC') in Schedule 4 of the *Migration Regulations*.[103] Relevantly these include meeting the character test,[104] and not being assessed by the Australian Security Intelligence Organisation ('ASIO') as a risk to security;[105] or subject to declarations or sanctions from the Foreign Minister.[106] For example, the Minister can declare that 'there is an unreasonable risk of an unwanted transfer of critical technology by the applicant'.[107] Failure to meet the character test under the *Migration Act* also enlivens a discretion to refuse or cancel any form of visa, including where that refusal or cancellation is 'in the national interest'.[108] In doing so, delegates of the Minister must consider the directions issued by the Minister under s 499 of the *Migration Act*,[109] but the Minister is not so bound when exercising those decisions personally. When a decision is rendered by the Minister personally, this has been considered a 'god-like power' because of

101 *Li* (n 1) [15]–[16], [60].

102 *Migration Regulations 1994* (Cth) sch 2, cl 408.226 ('*Migration Regulations*').

103 *Migration Act 1958* (Cth) s 31(3) ('*Migration Act*'); ibid reg 2.03(1), sch 4 pt 1.

104 *Migration Act* (n 103) ss 501(1), (6); *Migration Regulations* (n 102) sch 4 criterion 4001.

105 *Migration Regulations* (n 102) sch 4 criterion 4002.

106 Such as 'a person whose presence in Australia is, or would be, contrary to Australia's foreign policy interests' or 'a person whose presence in Australia may be directly or indirectly associated with the proliferation of weapons of mass destruction': ibid criteria 4003(a)–(b), 4003A.

107 Ibid criterion 4003B.

108 *Migration Act* (n 103) ss 501(1)–(3). Some cancellations 'must' or 'must not' be performed by the Minister or delegate if prescribed circumstances are met: *Migration Act* ss 134B; *Migration Regulations* (n 102) reg 2.43.

109 Minister for Immigration and Citizenship (Cth), *Direction No 99: Visa Refusal and Cancellation Under s501 and Revocation of a Mandatory Cancellation of a Visa Under Section 501CA* (23 January 2023).

the 'non-delegable, non-reviewable and non-compellable' nature of that decision.[110] A visa already granted may also be cancelled if any of the following apply:

- the holder might pose a risk to 'the health, safety or good order of the Australian community' or 'the health or safety of an individual or individuals';[111]
- the holder 'is not, or is likely not to be, a genuine student'[112]
- the holder 'has engaged, is engaging, or is likely to engage, while in Australia, in conduct (including omissions) not contemplated by the visa';[113] or
- 'there is an unreasonable risk of an unwanted transfer of critical technology by the holder of the visa'.[114]

An applicant fails the character test if, *inter alia,* he or she has or had membership or association with a 'group, organisation or person [who] has been or is involved in criminal conduct'[115] (broadly analogous to s 34(1)(f) of the Canadian *IRPA*). Another ground for failing the character test is where there is an apprehended risk that the person may 'engage in criminal conduct in Australia' or otherwise 'represent a danger to the Australian community or to a segment of that community, whether by way of being liable to become involved in activities that are disruptive to … that community or segment, or in any other way' (analogous to s 34(1)(b) of the *IRPA*).[116] A further ground is where 'the person has been assessed by the Australian Security Intelligence Organisation to be directly or indirectly a risk to security' (analogous to s 34(1)(d) of the *IRPA*).[117] Likewise, a determination by the Foreign Minister under PIC 4003 or 4003A, that the applicant is a risk to Australia's foreign policy interests and/or directly or indirectly associated with weapons of mass destruction, is fatal to an applicant's attempt to obtain a visa.[118]

Australian courts have traditionally limited migration reviews actuated by national security concerns to questions of law around legality, procedural fairness and reasonableness of decision-making, a position certainly far from ideal. Not only

110 Samuel C Duckett White, 'God-Like Powers: The Character Test and Unfettered Ministerial Discretion' (2020) 41(1) *Adelaide Law Review* 1; Aeron Leyesa and Janice Yong, '*Deus Ex* Minister: *Djokovic v Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs* (2022) 397 ALR 1' (2022) 43(2) *Adelaide Law Review* 961, 961.

111 *Migration Act* (n 103) s 116(1)(e).

112 Ibid s 116(1)(fa)(i).

113 Ibid s 116(1)(fa)(ii).

114 Ibid s 116(1)(g); *Migration Regulations* (n 102) reg 2.43(1)(c). This would potentially include the transfer of 'sensitive' technologies such as microfluidics to a country such as China.

115 *Migration Act* (n 103) s 501(6)(b).

116 Ibid s 501(6)(d).

117 Ibid s 501(6)(g), citing the definition of 'security' in the *Australian Security Intelligence Organisation Act 1979* (Cth) s 4 (which includes espionage) ('*ASIO Act*').

118 *Chen (Migration)* [2023] AATA 297; *Zhu v Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs* [2024] FedCFamC2G 411.

can it lead to confusing sets of circumstances where an appellant is left in the dark as to the likely grounds of any appeal or review,[119] it also renders the appeal of a visa refusal a functional nullity if the visa could not be granted because an adverse determination remains in place.[120] Further, it can mean that the courts must curtail the ordinarily expansive rights to procedural fairness in the interests of protecting the information or sources that demonstrated the security concerns.[121] And finally, it can result in judicial unwillingness to question matters of policy better left to the executive (as national security matters largely are).[122]

There are two reasons that this approach is relevant to research security. First, in respect of applicants who undergo a security assessment by ASIO, it is implicit in the Adverse Security Assessment ('ASA') process that the applicant will be assessed for risk of espionage (as well as all other forms of security threat). This is because the definition of 'security' in the *Australian Security Intelligence Organisation Act 1979* (Cth) ('*ASIO Act*') invokes the protection of the Commonwealth, States and Territories (and their people) from a wide range of conduct contrary to such security.[123] This includes acts of espionage, but also foreign interference, sabotage, as well as a catch-all to protect 'Australia's territorial and border integrity from serious threats' (without specifying what such threats might be).[124] Secondly, the *Migration Regulations* allow for the making of Ministerial determinations that an individual poses a risk for proliferation of weapons of mass destruction or — since the *Migration Amendment (Protecting Australia's Critical Technology) Regulations 2022* (Cth) ('*PACT Regulations*') took effect — of unreasonable risk of technology transfer that sit at a lower evidentiary threshold. Where ASIO does not issue an

119 *Leghaei v Director-General of Security* (2007) 241 ALR 141 ('*Leghaei*'). See also Leyesa and Yong (n 110) 967.

120 *SDCV v Director-General of Security* (2021) 284 FCR 357, 370 [44] (Bromwich and Abraham JJ) ('*SDCV*'). By contrast, in *CMA19 v Minister for Home Affairs* [2020] FCA 736 ('*CMA19*'), the Federal Court held that the Minister was wrong to deny a protection visa to a person who had served as an intelligence officer in the Liberation Tigers of Tamil Eelam, and potentially committed war crimes or crimes against humanity (thus failing the character test), on the grounds that he posed no risk to Australian society: at [1]–[8].

121 *Leghaei* (n 119). See also Keiran Hardy, 'ASIO, Adverse Security Assessments and a Denial of Procedural Fairness' (2009) 17(1) *Australian Journal of Administrative Law* 39, 39–44; Pauline Collins and Anthony Gray, '*SDCV v Director-General of Security*: Procedural Fairness and the Ability to Decide a Matter Based on Secret Evidence Not Disclosed to a Party or their Legal Team' (2024) 98(1) *Australian Law Journal* 57.

122 Amanda Sapienza, 'Justiciability of Non-Statutory Executive Action: A Message For Immigration Policy Makers' (2015) 79 *AIAL Forum* 70; John Logan, 'Not a Suicide Pact?: Judicial Power and National Defence and Security in Practice' (2022) 106 *AIAL Forum* 20; Greg Carne, 'The Legal Rhetoric of Safety and Security: Improving National Security Law Process, Enactment and Content by Moderating its Executive and Legislative Influence' (2023) 50(1) *University of Western Australia Law Review* 168.

123 *ASIO Act* (n 117) ss 4, 17, pt IV.

124 Ibid s 4 (definition of 'security').

ASA, or otherwise produces a security assessment favourable to the applicant, the Ministers of both immigration and foreign affairs have tremendous discretion to otherwise bar that applicant from Australia.

In *QDJM v Director-General of Security*, for example, a review was brought in the Administrative Appeals Tribunal by an applicant whose identity was protected.[125] The applicant had conducted research and provided material support at the instructions of an individual from the applicant's home country, where the applicant had assumed this individual was a member of his home country's intelligence services.[126] The applicant sought to dispute the ASA that ASIO produced about him on the basis that his conduct was not clandestine or deceptive,[127] was not conducted for 'intelligence purposes, or for the purpose of affecting political or governmental processes',[128] and was not 'otherwise detrimental to the interests of Australia'.[129]

The Tribunal disagreed, rejecting the applicant's submissions. Instead, the Tribunal found that the applicant's actions were motivated by instructions received from a foreign official to conduct property searches in Australia on Australian properties, and to deliver $20,000 to a person residing in Australia.[130] The Tribunal considered the applicant's conduct was both clandestine and deceptive, given that he undertook actions to comply with requests of a foreign government in circumstances that obscured the involvement of that same government.[131] The Tribunal was also satisfied that these acts were for 'intelligence purposes' because they were not done voluntarily, but at the behest of the foreign official (who the applicant knew was a member of a foreign intelligence service).[132] The Tribunal was satisfied that the applicant's conduct therefore affected Australia's national security.[133] The basis for the ASA was validated. A researcher, providing access to research data at the behest of a foreign intelligence service, may also fall under the same provisions as *QDJM* and be the subject of an ASA.

125 [2021] AATA 4761 ('*QDJM*').

126 Ibid [22]–[28].

127 Ibid [82]–[83].

128 Ibid [85], [87].

129 Ibid [85].

130 Ibid [68]–[70].

131 Ibid [79]. Foreign interference is any conduct that is 'clandestine or deceptive and [is] carried on for intelligence purposes [or] … carried on for the purpose of affecting political or governmental processes [or] are otherwise detrimental to the interests of Australia': *ASIO Act* (n 117) s 4.

132 A term not defined in the various Acts referenced in this article but given wide scope by the jurisprudence: *Jaffarie v Director General of Security* (2014) 226 FCR 505, 525 [64]–[65]; *SDCV* (n 120) 399 [175]; *QDJM* (n 125) [89]–[94].

133 *Criminal Code Act 1995* (Cth) sch 1, ss 90.4(2)(a), (f) ('*Criminal Code*'). The learned Tribunal Deputy President did not engage with whether the acts of foreign interference were 'detrimental to the interests of Australia', as it was not necessary for the Tribunal to consider that alternative submission: *QDJM* (n 125) [98].

When compared to the Canadian provisions in the *IRPA*, Australian migration law appears both broader in scope and more flexible in dealing with potential risks to research security by foreign nationals. The recent changes to the *PACT Regulations* likewise make clear that migration officials can (and should) have regard to the likelihood of breaches of research security during the visa process, by considering whether a student or researcher might pose an 'unreasonable' risk of unwanted technology transfer.[134] Given the above analysis and the paucity of literature on research security in Australia, what can *Li* teach our government and legal professionals about the use of migration law to control research security concerns?

V What Can Australia Learn From *Li*?

The first obvious difficulty with assessing *Li* in an Australian migration law context is that, unlike Canada, Australia has a statutory definition of espionage.[135] Given such a definition exists, judges may be somewhat constrained from widening the meaning of the word to take it beyond the context of the Acts in which it appears.[136] In Australia, where a judge might be invited to redefine the word espionage — such as by reference to it in an ASA or in the reasons of the Minister or their delegate — the term must be afforded a construction which gives effect to the object of the *Migration Act*,[137] being to 'regulate, *in the national interest*, the coming into, and presence in, Australia of non-citizens'.[138] The imposition of that national interest criterion has been held by the Federal Court of Australia to invoke a 'common thread' around 'the risk of harm posed by a person coming into or remaining in the Australian community'.[139] The question must be answered with respect to whether a refusal or cancellation decision 'lacked an evident and intelligible justification'.[140]

On that basis, there are a number of pathways that might plausibly be deployed to cater to an entrant in Mr Li's situation and evaluate the potential likelihood of a removal being properly grounded on those provisions. It can be assumed that a foreign individual like Mr Li, intending to undertake research or work in a sensitive and high-technology domain who has expressed a desire to return to his home country, would probably draw the attention of ASIO and be subject to a security

134 *Migration Regulations* (n 102) r 1.15Q, sch 4 criterion 4003B.

135 Not only under the *ASIO Act* (n 117), s 4, but also as a suite of discrete offences set out in *Criminal Code* (n 133) div 91 sub-divs A, B.

136 See the settled principles in: *Project Blue Sky Inc v Australian Broadcasting Authority* (1998) 194 CLR 355; *SGH Ltd v Federal Commissioner of Taxation* (2002) 210 CLR 51; *Alcan (NT) Alumina Pty Ltd v Commissioner of Territory Revenue (NT)* (2009) 239 CLR 27.

137 *Acts Interpretation Act 1901* (Cth) s 15AA.

138 *Migration Act* (n 103) s 4(1) (emphasis added).

139 *Roach v Minister for Immigration and Border Protection* [2016] FCA 750, [71], citing *Moana v Minister for Immigration and Border Protection* (2015) 230 FCR 367, 380 [58].

140 *Minister for Immigration and Citizenship v Li* (2013) 249 CLR 332, 367 [76].

assessment. Obviously, a prospective entrant that was the subject of an ASA would still likely see a visa application refused under s 501(6)(g) (unless the extant circumstances of their application warranted the Minister to not exercise their discretion to refuse the visa *à la CMA19*).[141] However, if one recalls the very expansive definition of 'security' in the *ASIO Act*[142] — and hence the various parameters towards which the inquiry of an ASA would be directed — a number of aspects of the entrant's history may be red flags from a research security perspective. After all, 'security' in the *ASIO Act* specifically includes 'protection of, and of the people of, the Commonwealth and the several States and Territories from … espionage',[143] as that term appears in the *Criminal Code*. 'Security' also includes protection from 'attacks on Australia's defence system' or 'acts of foreign interference'. Again, matters equally of relevance to acts intended to interfere with Australian research security. Thus, if ASIO formed the reasonable and real view that the entrant would pose a risk of espionage, attack on Australia's defence system, or foreign interference, ASIO would likely issue an ASA (resulting in the cancellation or refusal of the visa in question).

Of course, ASIO may decline to issue an ASA, particularly if they considered that the risk of an entrant being targeted or coerced on their return home was negligible or at least manageable. After all, it bears recalling that in *Crenna*, the Applicant's admission to Canada had in fact been cleared by the Immigration Department, the Minister's Office and CSIS.[144] So if an ASA was not issued in the case of our hypothetical entrant to Australia, the Minister would still have other means at his or her disposal if the Minister believed on reasonable grounds that the risk of espionage remained.

The Minister could conclude that the entrant's prior association with Beihang University — one of China's 'Seven Sons of National Defence' and an institution heavily involved with missile development for the PLA[145] — were matters of general conduct rendering him or her a person 'not of good character' under s 501(6)(c) of the *Migration Act*.[146] That seems a weak argument: to meet the criteria of poor character under s 501(6)(c) usually requires not only 'continuing conduct' but conduct of a kind 'that shows a lack of enduring moral quality'.[147] Given that mere association with a questionable institution was not deemed enough to warrant

141 *CMA19* (n 120).

142 *ASIO Act* (n 117) s 4.

143 Ibid s 4(a)(i) (definition of 'security').

144 *Crenna* (n 36) [44]–[50].

145 Australian Strategic Policy Institute, *Beihang University* (Web Page, 2019) <https://unitracker.aspi.org.au/universities/beihang-university/>.

146 *Wong v Minister for Minister Immigration and Multicultural Affairs* [2002] FCAFC 440, [33]. It also permits the consideration of conduct which occurs outside Australia: *DVE18 v Minister for Home Affairs* [2019] FCA 1389, [75]–[77].

147 *Godley v Minister for Immigration and Multicultural and Indigenous Affairs* (2004) 83 ALD 411, 426 [51]; cited in *Asare Appiah Johnson and Minister for Immigration, Citizenship, and Multicultural Affairs* [2023] AATA 251, [140].

inadmissibility under the *IRPA*,[148] I suggest it would equally fail to satisfy s 501(6)(c) of the *Migration Act*.[149]

As a ground for refusal, relying on an entrant's membership or association with a group or organisation that 'has been or is involved in criminal conduct'[150] is objectively less likely to fail. Section 501(6)(b) of the *Migration Act* does not require the Minister to consider whether the association or membership of the organisation colours the character of the applicant; membership or association under this statutory criteria is enough.[151] The Minister need only form a reasonable suspicion that a group or organisation has been or is engaging in criminal conduct (such as espionage), and then the Minister must make a finding of fact that the entrant was or is a member or associate of that entity.[152] The Minister's suspicion of criminal conduct does not require a conviction or court finding, merely an assessment of past facts to determine whether the association is 'innocent or culpable'.[153]

Indeed, based on the case of *Zhu* mere association seems capable of grounding a refusal decision.[154] On 8 June 2020, Xiaolong Zhu, a PhD student at the Queensland University of Technology, was deemed 'a person whose presence in Australia may be directly or indirectly associated with the proliferation of weapons of mass destruction (WMD)' by the Foreign Minister under PIC 4003(b), perhaps because of his prior association with Beihang.[155] Mr Zhu's review in the Administrative Appeals Tribunal and then the Federal Circuit and Family Court of Australia was unsuccessful. His Honour Egan J held that, as the WMD determination had not been revoked by the Foreign Minister, the applicant failed to meet the public interest criterion applying to the student visa under the *Migration Regulations* irrespective of whether or not he also demonstrated that he met the character test in s 501.[156] Meeting the character test and the adverse determination by the Foreign Minister were held to be separate considerations in the issue of a visa, such that

148 *Geng v Canada (Citizenship and Immigration)* [2023] FC 773.

149 Association with a university with strong defence ties also has no requisite grounding with the section in accordance with the Ministerial direction: Minister for Immigration and Citizenship (n 109) annex A section 2 cl 5(1)–(3).

150 *Migration Act* (n 103) s 501(6)(b); *Mrishaj v Minister for Immigration and Border Protection* (2016) 247 FCR 224.

151 '[T]he Minister is not required to further ruminate about whether a person's association with a group or organisation "has a bearing" on the person's character': *Stevens v Minister for Immigration and Border Protection* (2016) 153 ALD 346, 372 [102]. Cf *Haneef v Minister for Immigration and Citizenship* (2007) 161 FCR 40, 81 [230].

152 *Godley* (n147) 425 [47]; not disturbed on appeal: *Minister for Immigration & Multicultural & Indigenous Affairs v Godley* (2005) 141 FCR 552.

153 *NBMW v Minister for Immigration (No 2)* (2014) 222 FCR 376, 382–3, citing *Haneef* (n 151); *Re Patterson; Ex parte Taylor* (2001) 207 CLR 391. See also *Graham v Minister for Immigration and Border Protection* (2016) 246 FCR 439, 452 [58].

154 *Zhu* (n 118).

155 Ibid [3], [7], [10]–[15]. Cf Australian Strategic Policy Institute (n 145).

156 *Zhu* (n 118) [35].

there was no inconsistency in the Minister's delegate finding the applicant did not meet the PIC.[157]

Another foundation for visa refusal could also be based on ss 501(6)(d)(i) and (v) — the 'likelihood of criminal conduct' and/or 'likelihood of danger' grounds. Sub-sections 501(6)(d)(i) and (v) are cast in presumptive terms. It only considers possible future conduct by the visa applicant,[158] and the risk of that future conduct eventuating does not need to be a significant one.[159] Instead, these provisions consider the likelihood of conduct occurring which colours the applicant's character in a manner that affects the Minister's finding that they meet the character test. The criminal conduct contemplated by s 501(6)(d)(i) does not strictly require 'some temporal result, such as the incurring of a conviction',[160] though Ministerial Direction No 99 ('Ministerial Direction') makes clear that '[t]he reference to criminal conduct must be read as requiring that there is a risk of the person engaging in conduct for which a criminal conviction could be recorded'.[161]

However, the specific form of risk posed by Mr Li as outlined above was one of coercion and targeting by the intelligence services of his home country to reveal sensitive information he obtained during his PhD study. Those acts could be covered by the criminal provisions for espionage, foreign interference, and the theft of sensitive information or trade secrets in the *Criminal Code*,[162] and so allow the possible future conduct of the applicant to be assessed under s 501(6)(d)(i) in those terms. The Ministerial Direction makes clear that much of this provision is focused on 'the use of violence as a legitimate means of political expression',[163] but these are not the only matters the Minister may consider. However, the provision has

157 Ibid [36]. Cf *Plaintiff M47 v Director-General of Security* (2012) 251 CLR 1, 48 [71].

158 'Shortly put, persons who have committed or are likely to commit criminal or other like conduct should not be permitted to travel to or remain in Australia. Because the purpose is to exclude those persons, the matters that are relevant to the exercise of the Minister's discretion will include any fact or circumstance which would suggest that a person of otherwise bad character (as it is defined in the Act) should be allowed to travel to or remain in Australia': *Akpata v Minister for Immigration & Multicultural & Indigenous Affairs* [2004] FCAFC 65, 105.

159 '[I]f there is evidence suggesting that there is more than a minimal or remote chance': Minister for Immigration and Citizenship (n 109) annex A section 2 cl 6(2). The word 'significant' before the word 'risk' was removed by the *Migration Amendment (Character and General Visa Cancellation) Act 2014* (Cth) s 11.

160 *Minister for Immigration and Ethnic Affairs v Baker* (1997) 73 FCR 187, 194. In so doing, in the absence of a conviction the Minister's position on character 'will not be attained on slight material': at 194. See also *Tanielu v Minister for Immigration and Border Protection* (2014) 225 FCR 424, 450–1 [122]–[128].

161 Minister for Immigration and Citizenship (n 109) annex A section 2 cl 6.1(2).

162 *Criminal Code* (n 133) divs 91, 92, 92A.

163 Minister for Immigration and Citizenship (n 109) annex A section 2 cl 6.3(1).

previously been interpreted as involving activities which are disruptive or involve violence, threatening harm to the community or a segment of that community'.[164]

Yet there are some challenges with that approach. First, the chance of our hypothetical entrant's future offending materialising would still need to be more than likely — a refusal based on this provision will only be successful at administrative or judicial review if the Minister can successfully establish the requisite inter-relationship between the establishment of the occurrence of past events and the evaluation of the prospect that an event might occur in the future.[165] Such an assessment is evaluative,[166] and so may be hard to prove in the terms that were described in *Li*, where the reasonable ground for espionage was the applicant being targeted and coerced on his return to China during or after his studies. That said, being the target of such coercion could still ground reasonable suspicion of the commission of an offence, such as espionage — 'reckless as to national security',[167] 'recklessly supporting foreign intelligence agency',[168] or 'theft of trade secrets involving foreign government principal'.[169]

Second, the nature of the evaluation by the Minister is made more challenging when attempting to determine the threshold at which an individual would pose such a future risk (especially for a covert crime like espionage). In cases of criminal offending — where statistical tests and psychological assessments may be undertaken on convicted criminals to assess the likelihood of their reoffending for that purpose[170] — criminal histories are usually used to demonstrate future risk,[171] and Mr Li did not have one. However, the language of the statute (particularly in

164 *BHL19 v Minister for Immigration, Citizenship and Multicultural Affairs* (2019) 166 ALD 284, 300 [72]–[73]; *Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs v ERY19* (2021) 285 FCR 540, 561–3 [81]–[87]. Cf *LLSY and Minister for Immigration and Citizenship* (2011) 55 AAR 57.

165 *Minister for Immigration and Ethic Affairs v Guo* (1997) 191 CLR 559, 574–5.

166 *Madafferi v Minister for Immigration and Multicultural Affairs* (2002) 118 FCR 326, 353 [89]; *Minister for Immigration and Border Protection v Sabharwal* [2018] FCAFC 160, [2].

167 Where 'the person deals with information or an article; and the person is reckless as to whether the person's conduct will prejudice Australia's national security; and the conduct results or will result in the information or article being communicated or made available to a foreign principal or a person acting on behalf of a foreign principal': *Criminal Code* (n 133) s 91.2(2).

168 Where 'the person provides resources, or material support, to an organisation or a person acting on behalf of an organisation; and … the organisation is a foreign intelligence agency': ibid s 92.8.

169 Ibid s 92A.1(1).

170 See, eg, *CYTH and Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs (Migration)* [2020] AATA 2940, [155].

171 *QKVH and Minister for Home Affairs* [2020] AATA 4431; *Sadiq and Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs (Migration)* [2021] AATA 80.

s 501(6)(d)(v)) permits the Minister to take a 'pessimistic' and 'overly cautious' view of future offending, as the *Migration Act* 'is cast in terms that authorised the Minister to be highly protective of the Australian community when it [comes] to granting or refusing a visa when character is in issue'.[172] On that basis, a properly evidenced and well-crafted set of reasons could give rise to a refusal of a visa under section 501(6)(d)(i) of the *Migration Act*, based on the low (but beyond nil or remote) risk of the applicant's commission of a national security offence at some time in the future.[173]

Third, a risk that a person could be targeted or coerced by their home country into revealing sensitive information (and therefore committing a potential national security offence) is a matter going back to security under s 4 of the *ASIO Act*. Once again, the likelihood of an ASA being issued is high (given publicly available statements by ASIO about the threat posed by China[174]), and the assessment is likely to canvas the likelihood of Li's risk of espionage, foreign interference and technology theft as matters going to security.[175] If an ASA is issued, the ground of refusal under s 501(6)(g) of the *Migration Act* is enlivened in far less contentious circumstances than reliance upon s 501(6)(d)(i). Alternatively, a security assessment from ASIO (even a qualified assessment) that finds the applicant is *not* a threat to security would remain a highly relevant matter that weighs against a finding that the applicant poses a danger to the Australian community.[176]

The last matter for consideration involves recent developments by Australia to counter precisely the kinds of conduct that Li could have engaged in, quite separate from the application of the character test. From 1 July 2022, the *PACT Regulations* amendment took effect. The *PACT Regulations* amended the *Migration Regulations* by inserting a new PIC for the Minister to cancel a visa if the Minister was reasonably satisfied the visa holder posed 'unreasonable risk of unwanted critical

172 *BHL19 v Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs* (2020) 277 FCR 420, 490 [338]. See also *Falzon v Minister for Immigration and Border Protection* (2018) 262 CLR 333.

173 *Singh v Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs* [2022] FCA 1046, [43]–[44].

174 Jade Macmillan and Andrew Greene, 'ASIO Director Tells Five Eyes Intelligence Summit That Alleged Chinese Spy Was Removed from Australia', *ABC News* (online, 18 October 2023) <https://www.abc.net.au/news/2023-10-18/five-eyes-spy-summit-asio-cia-fbi-san-francisco/102984976>; Zeba Siddiqui, 'Five Eyes Intelligence Chiefs Warn on China's "Theft" of Intellectual Property', *Reuters* (online, 19 October 2023) <https://www.reuters.com/world/five-eyes-intelligence-chiefs-warn-chinas-theft-intellectual-property-2023-10-18/>; Evelyn Manfield, '"Disgruntled Employees" Being Targeted by Foreign Spies on Dark Web, As Insider Threats Become Major National Security Focus', *ABC News* (online, 1 November 2023) <https://www.abc.net.au/news/2023-11-01/criticial-infrastructure-review-finds-insider-espionage-threat/103048752>.

175 *ASIO Act* (n 117) s 4.

176 *DLF16 v Minister for Immigration and Border Protection* [2017] FCA 1072, [57]–[65].

technology transfer'.[177] A person poses such a risk if they could or might transfer (verbally or otherwise) a technology or any information about that technology that would 'harm or prejudice the security or defence of Australia', 'harm or prejudice the health and safety of the Australian public or a section of the Australian public', 'interfere with or prejudice the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth', or 'harm or prejudice Australia's international relations'.[178]

There has been little time for courts and tribunals to consider these new provisions. That said, the Minister would need to make several findings to enliven a refusal ground under PIC 4003B. The first would be a finding that the named technology — in Mr Li's case, microfluidics — was on the prescribed list.[179] The second finding is whether the entrant posed a risk of 'unwanted technology transfer' by providing microfluidics technology in a manner that met one or more of the criteria in the *Migration Regulations*, such as by 'enabling critical technology to be used in a way that is contrary to Australia's international obligations or commitments'.[180] The Minister would need to be satisfied, and articulate in reasons, the precise international obligation or commitment that the technology could contravene. A less obvious and perhaps weaker argument might also focus on the effect of 'prejudice' to the health of the Australian public,[181] especially given this same prejudice was the focus of the CFC in the application of microfluidics being against Canada's interests.[182]

For the preceding reasons, had an entrant like Mr Li applied for a visa to research in Australia, there would have certainly been several potential grounds for refusal. The most likely and efficient pathway is the conduct of a security assessment by ASIO and potential issue of an ASA, enlivening refusal under s 501(6)(g). Otherwise, the matter falls to ministerial discretion, such as whether the Minister was satisfied that the entrant's association with Beihang University and/or risk of his committing a national security offence like espionage, foreign interference or theft of trade secrets rendered him not of good character under s 501(6), or that he posed an unreasonable risk of unwanted technology transfer in the field of microfluidics under the *PACT Regulations* and PIC 4003B. Of course, such findings would depend entirely on the

177 *Migration Regulations* (n 102) sch 4 pt 1 criteria 4003B. Schedule 8, cl 8204 also prohibits the holder of a sub-class 500 Student Visa from changing their course of study or thesis without permission from the Minister.

178 Ibid regs 1.15Q(1)(c)–(f).

179 Microfluidics is not specifically listed, though could be captured as an 'advanced manufacturing and materials technology' because it 'produces, forms, shapes or structures matter in forms with one or more definable properties, characteristics, qualities, or features, and the results thereof': ibid regs 1.03, 1.15Q(2); *Migration (Critical Technology — Kinds of Technology) Specification* (LIN 24/010) 2024.

180 *Migration Regulations* (n 102) r 1.15Q(1)(f)(ii).

181 Ibid reg 1.15Q(1)(d).

182 *Li* (n 1) [55], [76].

information that was available to the Minister's delegate at the time of making the decision.[183]

Australia's *Migration Act* thus appears *prima facie* capable of rendering a decision similar to the CFC in *Li* and supporting the protection of research security in Australia. The definition of espionage which the Chief Justice of the CFC outlined — 'that Mr. Li may be recruited or coerced by the PRC to engage in the espionage activities [outlined]'[184] — itself falls within both the criminal statutory definitions and the case law of decided migration cases which have considered the risks of espionage and foreign interference in Australia as a basis for refusing visas. Yet there is also apparent parliamentary intent to capture precisely the kind of conduct Mr Li could have engaged in by virtue of the passage of the *PACT Regulations*, showing the Australian legislature has clearly been alive to the potential risk of these sorts of issues.

VI Conclusion

Li was considered a controversial decision in Canada because it involved an expansion of a common law definition of espionage which, until that time, had stringently focused on conduct involving information collection that was secret, clandestine, surreptitious or covert.[185] That same definition has clear implications for students and researchers working with Canadian universities, by applying potential findings of espionage to the sharing of any of their research data with foreign intelligence or government officers. However Canadian government policy has, to a significant extent, placed an *ex ante* restriction on such collaborations where the applicant has had affiliations with an entity on the NRO list. The broader impacts of this policy decision are yet to be examined; however, it is clear that academic freedom will be infringed, as will numerous projects with economic, social and cultural benefits to Canada.

Indeed, one of the key issues that *Li* and the broader research security framework in Canada highlights for Australia is the need for a comprehensive national policy position on research security. In the current environment, a lack of governmental

183 It bears repeating that the Minister may exercise their discretion to cancel the visa if the person does not meet the character test and it is otherwise 'in the national interest': *Migration Act* (n 103) s 501(3). Such 'national interest' may be met with consideration of the risk of technology transfer by the applicant, such as are outlined in the *Migration Amendment (Protecting Australia's Critical Technology) Regulations 2022* (Cth).

184 *Li* (n 1) [63].

185 Will Tao, 'Part 2A — An Annotated Review of Li and the Unforeseen and Unsettled Legal Consequences of Expanding the Definition of Espionage', *Vancouver Immigration Blog* (Blog Post, 11 January 2024) <https://vancouverimmigrationblog.com/li-fc-espionage-part2a/>; Steven Muerrens, 'The Expansion of Inadmissibility for Espionage', *Muerrens on Immigration* (Blog Post, 17 January 2024) <https://meurrensonimmigration.com/the-expansion-of-inadmissibility-for-espionage/>.

certainty about the application of research security provisions in Australian university research and development is incredibly short-sighted. Whilst Australia does not need to go as far as Canada in erecting a named list of prohibited institutions, it certainly could do so and would join other Western nations like the United States and Japan.[186]

In Australia's defence, the *PACT Regulations* demonstrate the legislature's intention to proscribe precisely the form of conduct that research security is targeted towards: the collection of information or material that touches upon advanced technologies and is disclosed to a foreign nation to the detriment of Australia or Australia's interests. These changes to Australian immigration laws will enable the Minister to have a clearer pathway to refusing potential risks to Australia's higher education research sector. Where the *PACT Regulations* do not apply, ASIO security assessments and the character test in s 501(6) of the *Migration Act* remain highly useful tools to support the objects of the Act in determining the entry status of non-citizens to Australia in a manner that meets the public interest.

There are some matters which could warrant further scrutiny and research, both by the legal profession and the academic community. The first is that the *PACT Regulations* require the Minister to publish an instrument defining the term 'critical technology'.[187] Although a reasonable assumption would be to suggest that such an instrument would prescribe anything on the *List of Critical Technologies in the National Interest*[188] (which includes artificial intelligence, quantum technologies, biotechnology and clean energy generation and storage), as well as any of the military or dual-use technologies listed on the *Defence and Strategic Goods List 2024* (Cth),[189] these lists do not completely overlap. Where a technology is in the national interest but is not proscribed in the Minister's declaration, the PIC 4003B criterion cannot be relied upon in refusal or cancellation decisions, meaning that Australia lacks access to one of the most useful tools in regulating the types of conduct described in *Li*.

The Direction could also be amended to contemplate past actions of a visa applicant or holder that run counter to Australia's interests.[190] Currently, Australian interests

---

186 See, eg: Bureau of Industry and Security, *Lists of Parties of Concern* (Web Page) <https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern>; Ministry of Economy, Trade and Industry, *Review of the End-User List* (Web Page, 6 December 2023) <https://www.meti.go.jp/english/press/2023/1206_001.html>.

187 *Migration Regulations* (n 102) regs 1.03, 1.15Q(2). Currently the Migration (Critical Technology — Kinds of Technology) Specification (LIN 24/010) 2024.

188 Department of Industry, Science and Resources, *List of Critical Technologies in the National Interest* (Web Page, 19 May 2023) <https://www.industry.gov.au/publications/list-critical-technologies-national-interest>.

189 Made under the *Customs Act 1901* (Cth) s 112(2A)(aa) and enforceable by the *Defence Trade Controls Act 2012* (Cth).

190 This matter was raised but not considered by the Administrative Appeals Tribunal in *QDJM* (n 125) [106]–[108].

do not have the same level of statutory recognition as Canadian interests do in the *IRPA*. Whilst such matters are considered by ASIO in the conduct of a security assessment,[191] ASIO may reach a conclusion that the applicant or holder does not pose a risk to Australia's security. In such cases, the Department of Home Affairs should be permitted the widest possible scope to consider the relevant risks which may be posed by a potential arrival into Australia. Without a clear recognition of Australia's interests in the underpinning document for use in such decisions, it is entirely possible that one day a decision may be made that compromises those very same interests.

Finally, there will need to be a groundswell in research on the unintended implications of these controls on the notions of open collaboration, freedom of expression and publication of results that are the hallmarks of Western universities. These discussions in the literature are still very much in their infancy, and somewhat *ad hoc* in their approach and focus.[192] Not only will further research provide a more nuanced understanding of the contours of academic freedom, but it will ensure that academic institutions — especially in the West — do not end up aping the draconian control systems of the very nation-States they are attempting to protect themselves against.

191 Australian interests are imported into 'acts of foreign interference' in *ASIO Act* (n 117) s 4, and thus become a matter of 'security'. An ASA will enliven s 501(6)(g) and inform a refusal or cancellation.

192 Grubbs (n 8); Shih (n 11); Robert Schaefer, 'Academic Freedom and International Students, Part 5: The Gray Areas' (2024) 49(2) *ACM SIGSOFT Software Engineering Notes* 10.