THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

CREATE CHANGE

27 November 2020

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Canberra ACT 2600

To the Committee,

Inquiry into national security risks affecting the Australian higher education and research sector

Thank you for the opportunity to make a submission to this Inquiry. We do so jointly as members of the University of Queensland School of Law. We are solely responsible for the views and content of this submission.

Our submission is limited to Term of Reference C:

> *The adequacy and effectiveness of Australian Government policies and programs in identifying and responding to foreign interference, undisclosed foreign influence, data theft and espionage in the Sector.*

In particular, we address the adequacy of existing espionage laws in this context.

Our primary point for the Committee's attention is that Australia's existing espionage laws are adequate to address the threat of modern espionage. Moreover, their breadth and complexity risks undermining basic rights and freedoms and criminalising innocent conduct.

This analysis draws on research published in:

- Sarah Kendall, 'Australia's Espionage Laws: Another Case of Hyper-Legislation and Over-Criminalisation' (2019) 38(1) *University of Queensland Law Journal* 125 (*Annexure A*), and
- 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* (forthcoming).

The University of Queensland
Brisbane QLD 4072 Australia
T [redacted]
M [redacted]
E [redacted]
W law.uq.edu.au
ABN: 63 942 912 684
CRICOS PROVIDER NUMBER 00025B

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
CREATE CHANGE

1. Australia's espionage offences are adequate to address the threat of modern espionage

Australia has a complex suite of 27 espionage offences in Division 91 of the *Criminal Code Act 1995* (Cth). A Table summarising these offences can be seen on page 143 of the attached article.

1.1 The Reach of Australia's Underlying Espionage Offences

Australia's espionage offences criminalise *dealings* with *information or articles* on behalf of, or to communicate to, a *foreign principal*. Some of the offences also require that the person intends (or is reckless to) their conduct prejudicing Australia's *national security*, or giving advantage to the national security of a foreign country.

These key terms are defined broadly, giving the provisions an effective reach over modern espionage activities:

- *Deals with* is defined to include receiving, obtaining, collecting, possessing, making a record, copying, altering, concealing, communicating, publishing or making available.[i]
- *Information* means 'information of any kind, whether true or false and whether in a material form or not, and includes an opinion, and a report of a conversation'.[ii]
- *Articles* means 'any thing, substance or material'.[iii]

Dealing with information or articles encompasses dealing with all or part of such, or even its 'substance, effect or description'.[iv]

These definitions mean the espionage offences encompass the wide variety of ways in which information is handled in the higher education and research sector ('the Sector'), extending not only to research in written forms, but also ideas, thoughts or discussions about research, as well as the physical products of research (such as vaccines, technologies and materials).

The core espionage offence, in section 91.1 of the *Criminal Code*, requires that the information be of a certain type, namely, national security or security classified information.

Security classified information has a formal security classification of Secret or Top Secret. Such information is rarely the subject of research in the Sector – though if it were (say in research conducted on behalf of, or in relation to, defence or intelligence agencies) the researcher's handling of that information may satisfy the physical elements of the core espionage offence or classified information espionage (in section 91.3 of the *Criminal Code*).

National security information, however, is far broader and is regularly handled by researchers in the Sector.

National security information may concern: defence of the country; protection of the country's borders from serious threats; protection of the country from activities such as espionage, sabotage, terrorism, and foreign interference; the carrying out of a country's responsibilities to any other country; and a country's political, military or economic relations with another country.[v] The core espionage offence may therefore impact research into defence and intelligence, as well as certain areas of law, political science, economics, and international relations.

The espionage offences further require that the information was dealt with on behalf of, in collaboration with or under the direction, funding or supervision of a *foreign principal*, or that the dealing will result in communication to a foreign principal.

Foreign principal means foreign governments or authorities (including local governments), foreign political organisations, public international organisations, terrorist organisations, foreign public enterprises (essentially entities controlled by foreign governments), and entities owned, directed or controlled by any of these foreign principals.[vi]

Therefore, it is not necessary that espionage against the Sector be conducted by a foreign state – it could be engaged in by a foreign government-controlled corporation, political organisation of a foreign country that is not currently in power, or a terrorist group.

The publication of research findings – for instance, in an academic journal, book, or online – would amount to '*communication to a foreign principal*' for the purposes of the espionage offences. This means that the publication of academic research on Australia's economic relations with foreign countries in an academic journal would amount to dealing with national security information for the purpose of communication to a foreign principal – satisfying the physical elements of the core espionage offence. So too would communication of such information to a foreign intelligence agency by a person engaged in espionage against the Sector.

In addition to these physical elements, the espionage offences in sections 91.1, 91.2 and 91.8 require the person to satisfy certain *mental elements*. Specifically, it must be proved that the person intended to (or was reckless as to whether their conduct would):

- prejudice Australia's national security, or
- advantage the national security of a foreign country.

Prejudice has been defined only so that 'embarrassment alone is not sufficient to prejudice' national security[vii] – meaning anything above mere embarrassment could satisfy this element. Furthermore, recklessness only requires that the person was aware of a substantial risk and it was unjustifiable for them to take that risk in the circumstances.[viii]

It is possible for any or all of these mental elements to be satisfied where someone engages in espionage within or against the Sector, particularly where there is a risk that the information could harm Australia or advantage another country in some way (such as if the research material related to new military technologies, trade secrets, or a vaccine). There is also a risk that academic outputs and actions which fall outside traditional conceptions of espionage, but which recklessly prejudice Australia's international relations, could amount to espionage under Australia's current laws.

A notable inclusion in the espionage offences is the 'theft of trade secrets involving foreign government principal' (trade secrets espionage) in Division 92A of the *Criminal Code*. Trade secrets espionage specifically criminalises the theft of trade secrets where this is done on behalf of or is funded by a foreign government principal.[ix] It does not include a mental element. This offence is particularly relevant to the Sector, where trade secrets may be stolen to assist state-sponsored

foreign entities skip or accelerate the research and development phase of product development, which ultimately benefits the country's economy.

1.2 Extended Criminality: Espionage-Related Offences

Australia's espionage scheme further includes solicitation and preparatory offences. These offences criminalise the earliest stages of criminal conduct.

The *solicitation offence* criminalises an intention to solicit or procure, or make it easier to solicit or procure, an espionage offence where this is done on behalf of a foreign principal.[x] This offence criminalises the conduct of recruiters of spies and could prove useful in circumstances where Australian researchers are targeted for information. It is not necessary that the researcher actually have committed an espionage offence or for such conduct to even be possible.[xi]

The *preparatory offence* criminalises preparing for or planning an espionage offence[xii] and also arises where an espionage offence has not been committed.[xiii] This is the broadest of the espionage offences and resembles the catch-all 'preparing for or planning terrorist acts' offence found in section 101.6 of the *Criminal Code*.

The *inchoate liability* provisions of the *Criminal Code* also apply to this offence (with the exception of attempt) which creates, for example, the offence of *conspiracy to prepare* for espionage. This offence criminalises pre-preparatory conduct, such as merely agreeing to prepare for espionage in the future. These two offences – the preparatory offence and conspiracy to prepare for espionage – give Australia's espionage framework a particularly broad scope, so that suspects may be arrested prior to information being collected or communicated.

We note that the similar offence of 'conspiracy to do an act in preparation for a terrorist act' has supported numerous terrorism prosecutions, but has attracted criticism for it's unusual breadth and risk to fundamental rights and liberties.[xiv]

1.3 Conclusion

Australia's espionage offences are more than adequate to address the threat of espionage faced by the Sector. Their physical elements encompass the breadth of ways in which information is handled for, and communicated to, foreign entities in the higher education sector.

2. Law reform options should be considered in light of recognised issues with the existing espionage offences

Our primary submission is that legislative change to the espionage offences is not necessary to address the new and emerging threats considered by this Inquiry. If law reform is considered, however, then it should be approached with caution.

The espionage offences are highly complex. Unlike the United Kingdom, which only has three espionage offences,[xv] Australia has a complicated scheme of 27 different offences. These include nine underlying offences, two espionage-related offences and 16 aggravated offences (that arise

from a combination of four aggravated circumstances and four underlying offences).[xvi] Three defences exist, but they do not apply to all offences. Furthermore, each of the underlying offences utilises similar key terms, and differ only slightly in the elements that must be established. This means that certain conduct may fall within a number of the espionage offences and be easier to prove under one offence compared to another.

The espionage offences are both broad and uncertain in their scope. For example, *deals with* includes mere passive receipt of information, *national security* includes international and economic relations, *information* includes false information and opinions, and *prejudice* has not been effectively defined. The breadth of the offences means that conduct that should not be criminalised – such as certain journalistic conduct, or innocent preparatory conduct – may in fact be criminalised. This can have unintended consequences, such as a chilling effect on free speech.

In the Sector, there is a risk that legitimate research with no connection to a foreign entity may amount to espionage. For instance, an espionage offence may be committed where research findings could prejudice Australia's international relations, and those findings are published in an academic journal capable of being accessed by the public (which includes foreign states). Uncertainty over the scope of the espionage laws could therefore stifle free speech and independent research.

In **summary**, we submit that:

1. Australia's espionage offences are adequate to address the threat of modern espionage.
2. Law reform should be approached cautiously, in light of recognised issues with the existing espionage offences.

Yours sincerely

Sarah Kendall
PhD Candidate
University of Queensland, School of Law

Dr Rebecca Ananian-Welsh
Senior Lecturer
University of Queensland, School of Law

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
CREATE CHANGE

Attachments

- Sarah Kendall, 'Australia's Espionage Laws: Another Case of Hyper-Legislation and Over-Criminalisation' (2019) 38(1) *University of Queensland Law Journal* 125-161.

References

[i] *Criminal Code 1995* (Cth) s 90.1(1) (definition of 'deal').
[ii] Ibid (definition of 'information').
[iii] Ibid (definition of 'article').
[iv] Ibid s 90.1(2).
[v] Ibid s 90.4.
[vi] Ibid ss 90.2, 90.3, 70.1.
[vii] Ibid s 90.1(1) ('definition of 'prejudice').
[viii] Ibid s 5.4.
[ix] Ibid s 92A.1.
[x] Ibid s 91.11.
[xi] Ibid s 91.11(3).
[xii] Ibid s 91.12.
[xiii] Ibid s 91.12(3).
[xiv] Independent National Security Legislation Monitor, Commonwealth of Australia, *Annual Report 16 December 2011* (2012) 58; Andrew Lynch, George Williams and Nicola McGarrity, *Inside Australia's Anti-Terrorism Laws and Trials* (NewSouth, 2015) 32, 35-9.
[xv] See *Official Secrets Act 1911* (UK) s 1(1).
[xvi] See the table of Underlying Espionage Offences in Sarah Kendall, 'Australia's Espionage Laws: Another Case of Hyper-Legislation and Over-Criminalisation' (2019) 38(1) *University of Queensland Law Journal* 125, 143.

AUSTRALIA'S NEW ESPIONAGE LAWS: ANOTHER CASE OF HYPER-LEGISLATION AND OVER-CRIMINALISATION

SARAH KENDALL*

Australia introduced its first espionage offence in 1914. This was repealed in 2002 and replaced with four new offences. Just 16 years later, these offences have again been the subject of legislative change; in June 2018, they were repealed and replaced with 27 new offences. Justifications for the introduction of both the 2002 and 2018 offences were on the grounds that existing offences (relevantly the original 1914 offence or the 2002 offences) failed to capture modern espionage practices, deter espionage activity and secure convictions. Examination of the original and 2002 offences demonstrated that, in these respects, those offences failed to address espionage used today. The 2018 offences, however, remedy that failure and are therefore necessary to effectively address espionage used in today's world. Despite this, the broad nature of conduct criminalised by some of the offences raises concerns over criminalisation of conduct that may have an innocent explanation. Further concerns arise over the number and overlapping nature of the new offences. Discussion of these issues may provide useful insights for movements toward law reform in the United Kingdom and other Five Eyes nations.

I INTRODUCTION

Espionage has been defined as 'the practice of spying or using spies, typically by governments to obtain political and military information'.[1] It has been used by nations throughout the ages to gather information on foreign states, with records of espionage dating as far back as Biblical times.[2] Espionage is considered necessary when performed by one's home country for the purposes of national

* TC Beirne School of Law, University of Queensland. The author would like to thank Rebecca Ananian-Welsh and the anonymous reviewers for their invaluable comments on previous drafts.

1 *Oxford English Dictionary* (online at 21 June 2019) 'espionage'.

2 Darien Pun, 'Rethinking Espionage in the Modern Era' (2017) 18 *Chicago Journal of International Law* 353, 355; Terry Crowdy, *The Enemy Within: A History of Espionage* (Osprey Publishing, 2006) ch 1.

security and unacceptable where it involves foreign nations spying on that country.[3] The latter is traditionally criminalised.[4]

Australia introduced its first national espionage offence in 1914 with the *Crimes Act 1914* (Cth) ('*Crimes Act*').[5] This offence was repealed in 2002 and replaced with four new offences[6] found in the *Criminal Code Act 1995* (Cth) ('*Criminal Code*').[7] These new offences increased the maximum penalty from seven years' imprisonment to 25 years' imprisonment for all offences.[8] In June 2018, the Federal Parliament pushed through the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth) ('*Espionage Act*') within three days.[9] This Act repealed the four existing espionage offences and replaced them with 27 new offences.[10] Not only are these offences broader than previous offences, but many penalties are also more severe. Interestingly, in 2017 the United Kingdom Law Commission recommended that changes be made to the United Kingdom's espionage laws that closely resemble the amendments made in Australia;[11] however, these reforms have been widely criticised by the media[12] and have not yet been implemented.

The rationale behind the introduction of Australia's 2002 espionage offences was to 'better deter and punish those who intended to betray Australia's security interests' and to reflect the 'modern intelligence environment'.[13] Similarly, the 2018 offences were justified on the basis that the 2002 offences were too narrow

---

3 Pun (n 2) 355.

4 Ibid.

5 *Crimes Act 1914* (Cth) s 78 ('*Crimes Act*'), as repealed by *Criminal Code Amendment (Espionage and Related Matters) Act 2002* (Cth) sch 1 items 1, 5 ('*Espionage and Related Matters Act*').

6 See *Espionage and Related Matters Act* sch 1 items 1, 5.

7 *Criminal Code Act 1995* (Cth) s 91.1 ('*Criminal Code*'), as repealed by *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth) sch 1 item 17 ('*Espionage Act*').

8 *Crimes Act* s 78(1), as repealed by *Espionage and Related Matters Act* sch 1 items 1, 5; *Criminal Code* s 91.1, as repealed by *Espionage Act* sch 1 item 17.

9 National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018 (29 June 2018) <https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6022>.

10 See *Espionage Act* sch 1 item 17.

11 See United Kingdom Law Commission, *Protection of Official Data: A Consultation Paper*, Consultation Paper No 230 (2017).

12 See, eg, Roy Greenslade, *UK's Proposed Espionage Act will Treat Journalists like Spies* (17 March 2017) Committee to Protect Journalists <https://cpj.org/blog/2017/03/uks-proposed-espionage-act-will-treat-journalists-.php>; Duncan Campbell, 'Planned Espionage Act Could Jail Journos and Whistleblowers as Spies', *The Register* (online), 10 February 2017; EDRi, *Proposed Espionage Act Threatens Free Speech in the UK* (22 February 2017) <https://edri.org/proposed-espionage-act-threatens-free-speech-in-the-uk/>.

13 Revised Explanatory Memorandum, Criminal Code Amendment (Espionage and Related Matters) Bill 2002 (Cth) 1, 5.

and had failed to evolve with the modern threat environment.[14] Then Prime Minister Malcolm Turnbull stated during the 2018 Espionage Bill's second reading speech that 'our espionage laws are so unwieldy that they have not supported a single conviction in decades, even as the threat [of espionage] reaches unprecedented levels'.[15] Justifications for the introduction of both the 2002 and 2018 offences therefore appeared to be that existing offences failed to capture modern espionage practices, deter espionage activity or secure convictions. If the 2002 offences successfully remedied those issues to better address espionage threats, why were the 2018 offences necessary?

Naturally, law-making in the area of national security is highly political and often in response to national and international security incidents. While it is important to acknowledge that political dynamics may be the real reason behind introduction of the 2018 espionage offences, now that the offences have been introduced, it is vital to assess whether they meet their objective purpose. This article therefore examines whether the 2018 espionage offences are necessary to effectively address espionage used in today's world. First, it will explore typical espionage methods used during the major twentieth-century wars before discussing espionage practices used today, highlighting that today's espionage is characterised by cyber espionage. Second, it will compare the original and 2002 offences to determine whether the 2002 offences effectively captured today's espionage practices, deterred others from committing espionage and secured convictions. Third, the 2002 and 2018 offences will be compared to determine whether the newly introduced offences are likely to improve on the 2002 offences and will therefore be necessary to effectively address espionage practices used today. Both existing and anticipated problems with the 2018 offences, such as their broad scope, extensive number and complicated structure, will also be discussed. Finally, recommendations will be made to improve the 2018 offences. It will also be suggested that this analysis of Australia's new espionage offences could provide some useful insights for the United Kingdom in its endeavours to reform its espionage laws.

II What Is Espionage?

Espionage is 'the practice of spying on others … [—] the use by a government to discover the military and political secrets of another nation … [g]enerally [by] …

---

14 Revised Explanatory Memorandum, National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (Cth) 43 [16].

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

persons employed by a foreign power for that purpose';[16] it is 'the theft of Australian information by someone either acting on behalf of a foreign power or intending to provide information to a foreign power which is seeking advantage'.[17] One academic has pertinently described espionage as a 'clandestine state-sponsored intelligence-gathering operation, or series of operations, conducted through physical penetration into foreign territory ... or remote data collection techniques'.[18] It is just one of a number of different offences intended to protect Australia's national security interests.[19] Espionage differs from sabotage,[20] for example, which involves the deliberate destruction of or damage to things, although both may similarly involve a foreign power seeking to gain an advantage.[21] It also differs from 'foreign interference' as criminalised in 2018.[22] Although the espionage and foreign interference offences are intended to complement each other, foreign interference involves harmful conduct that falls short of espionage 'undertaken by foreign principals who seek to interfere with Australia's political, governmental or democratic processes, to support their own intelligence activities or otherwise prejudice Australia's national security'.[23] Discussion of the foreign interference offences is beyond the scope of this article.

While the concept of 'espionage' generally remains stable, its nature and practices continue to evolve. For this reason, it is not possible to comprehensively define past, present or future espionage practices. Changes have occurred (and will continue to occur) along a continuum and must be viewed in context. Despite this, for the purpose of analysing Australia's espionage laws, it will be useful to examine general trends in espionage practices across two time periods: the twentieth-century wars and today's world. This section will explore this, highlighting that espionage practices have largely been influenced by the technology available at the time. This analysis will allow core components of espionage practices used today to be identified, which can then be used to assess one aspect of the effectiveness of the 2002 and 2018 offences.[24]

---

16 *R v Lappas* [2003] ACTCA 21, [86].

17 Australian Security Intelligence Organisation ('ASIO'), *Counter-Espionage* (2018) <https://www.asio.gov.au/counter-espionage.html>.

18 Nicolas Jupillat, 'From the Cuckoo's Egg to Global Surveillance: Cyber Espionage that Becomes Prohibited Intervention' (2017) 42 *North Carolina Journal of International Law* 933, 953.

19 See Revised Explanatory Memorandum, National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (Cth) 2 [4].

20 See *Criminal Code* div 82.

21 *Oxford English Dictionary* (n 1) 'sabotage'.

22 See *Criminal Code* div 92.

23 Revised Explanatory Memorandum, National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (Cth) 3 [9], 43 [19].

24 That is, whether the offences are worded appropriately to capture espionage practices used in today's world. The other two factors that will be used to assess the offences' effectiveness are their ability to deter others from committing espionage and how frequently they did (or will) secure

A *Twentieth-Century Wartime Espionage*

Australia's original espionage offence was enacted in 1914[25] in the context of World War I and was not amended until 2002, long after World War II and the Cold War. The two World Wars saw both sides of each global conflict use traditional 'spies' to conduct espionage. These spies went undercover to gain knowledge and secrets about other countries' military capabilities and plans.[26] They often communicated in code or cipher and physically concealed messages in, for example, hollow walking sticks, the lining of clothing, soles of shoes and suitcases.[27] As technology progressed, these messages were sometimes communicated via short-wave radio transmitters or telephone.[28]

Spies themselves could be classified as 'legals' or 'illegals'.[29] 'Legals' were diplomats operating under diplomatic immunity who were able to collect information as a result of their status by, for example, visits to unrestricted sites.[30] They operated legally and used their diplomatic status as justification for their presence in foreign countries.[31] 'Illegals' posed as tourists, workers or students of English abroad, for example, or resided as 'locals' in the targeted country.[32] They

convictions. For a comprehensive account of the history of ASIO, see: David Horner, *The Spy Catchers: The Official History of ASIO, 1949–1963* (Allen & Unwin, 2014); John Blaxland, *The Protect Years: The Official History of ASIO, 1963–1975* (Allen & Unwin, 2015); John Blaxland and Rhys Crawley, *The Secret Cold War: The Official History of ASIO, 1975–1989* (Allen & Unwin, 2017). For a comprehensive account of the history of the United Kingdom's MI5, see Christopher Andrew, *The Defence of the Realm: The Authorised History of MI5* (Random House USA, 2010).

25 *Crimes Act* s 78.

26 Jupillat (n 18) 951–2; Luke Pelican, 'Peacetime Cyber-Espionage: A Dangerous but Necessary Game' (2012) 20 *CommLaw Conspectus* 363, 383; Jonathon Lewis, 'The Economic Espionage Act and the Threat of Chinese Espionage in the United States' (2009) 8 *Chicago-Kent Journal of Intellectual Property* 189, 189; Michael Sulick, *Spying in America: Espionage from the Revolutionary War to the Dawn of the Cold War* (Georgetown University Press, 2012) 167; Crowdy (n 2) chs 9, 13; see John Fox, 'What the Spiders Did: US and Soviet Counterintelligence before the Cold War' (2009) 11(3) *Journal of Cold War Studies* 206; Steven Usdin, 'The Rosenberg Ring Revealed: Industrial Scale Conventional and Nuclear Espionage' (2009) 11(3) *Journal of Cold War Studies* 91, 113–14.

27 See Usdin (n 26); Sulick (n 26) 173; Crowdy (n 2) chs 9–12; see James Gannon, *Stealing Secrets, Telling Lies: How Spies and Codebreakers Helped Shape the Twentieth Century* (University of Nebraska Press, 2001).

28 Usdin (n 26) 126; Jupillat (n 26) 963, 970–1; Sulick (n 26) 173, 272; see Crowdy (n 2) chs 9–13; Gannon (n 27) 141, 151.

29 Usdin (n 26) 126.

30 Kristin Vara, 'Espionage: A Comparative Analysis' (2015) 22 *ILSA Journal of International and Comparative Law* 61, 71–3; Sulick (n 26) 167, 175–6; Crowdy (n 2) chs 10, 13.

31 Vara (n 30) 71–3; Sulick (n 26) 167, 175–6; Crowdy (n 2) chs 10, 13.

32 Vara (n 30) 63, 71–3; see Usdin (n 26); Andrew Kim, 'Prosecuting Chinese "Spies": An Empirical Analysis of the Economic Espionage Act' (2018) 40 *Cardozo Law Review* 749, 752, 760; ASIO, *The Petrovs and Countering Cold War Espionage* (2018) <https://www.asio.gov.au/about/history/petrovs-and-countering-cold-war-espionage.html> ('*The Petrovs*'); Sulick (n 26) 167, 175–6; Crowdy (n 2) chs 10, 13.

were not protected by diplomatic immunity, but this lack of status meant that they could go largely undetected in the foreign country.[33] Some female spies were used as seductresses or in brothels to lure in foreign officials who would then be blackmailed for information.[34]

Similar practices were used during the Cold War, although advances in technology meant that the majority of messages were communicated wirelessly.[35] While satellites were increasingly being used to collect photographic or voice information,[36] the focus remained on traditional espionage by spies in the field.[37] The Soviet Union in particular had perfected such practices; Soviet spies had infiltrated every key agency of the United States' executive and legislative branches prior to the beginning of the Cold War, with a large spy ring active in Australia, too.[38] Corporations were also being used as fronts for stealing industrial secrets.[39] The focus of Soviet espionage during the Cold War was scientific research, particularly into development of the atomic bomb.[40]

B *Espionage in Today's World*

Espionage used today differs from twentieth-century wartime espionage in several key ways. Although traditional spies are still used (now generally referred to as 'intelligence officers' or employees of intelligence agencies), significant advancements in the sophistication and range of technology available have shifted the focus to cyber espionage.[41] Cyber espionage involves the use of technology to acquire information that would otherwise have to be collected by

---

33 Vara (n 30) 71–3; ASIO, *The Petrovs* (n 32); Sulick (n 26) 167, 175–6; Crowdy (n 2) chs 10, 13.

34 Crowdy (n 2) chs 10, 11.

35 Jupillat (n 26) 970–1; see Usdin (n 26); see Raymond Garthoff, 'Foreign Intelligence and the Historiography of the Cold War' (2004) 6(2) *Journal of Cold War Studies* 21; Sulick (n 26) 272; Crowdy (n 2) ch 13.

36 Garthoff (n 35) 24, 43–5.

37 ASIO, *The Petrovs* (n 32); Sulick (n 26) 272; Crowdy (n 2) ch 13.

38 ASIO, *The Petrovs* (n 32); see Fox (n 26); see Usdin (n 26); see Ellen Schrecker, 'Soviet Espionage in America: An Oft-Told Tale' (2010) 38(2) *Reviews in American History* 355; Sulick (n 26) 167; Crowdy (n 2) ch 13.

39 William Banks, 'Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage' (2017) 66 *Emory Law Journal* 513, 513–4; Vara (n 30) 66; Sulick (n 26) 167; Crowdy (n 2) ch 13.

40 Usdin (n 26); Schrecker (n 38) 355; Sulick (n 26) 167; Crowdy (n 2) ch 13.

41 Swatasoma Mohanty, 'Cyber Espionage — Burglary of the 21st Century' (2017) 109 *Intellectual Property Forum: Journal of the Intellectual and Industrial Property Society of Australia and New Zealand* 51; Pun (n 2) 355–6; Parliamentary Joint Committee on Intelligence and Security ('PJCIS'), Parliament of Australia, *Advisory Report on the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 17* (2018) 3, 203–4, 268; Commonwealth, *Parliamentary Debates*, House of Representatives, 7 December 2017, 13146 (Malcolm Turnbull); Max Mason, 'Spooks fear fake news threat to local election', *The Australian Financial Review* (Melbourne), 10 September 2018, 30; ASIO, *ASIO Annual Report 2017–18* (2018) 54.

human intelligence officers in the field.[42] Instead of stealing small pieces of information that must be assembled individually and 'assembled like a jigsaw', terabytes of data can be collected within seconds by an individual who has not left the safety of their home country.[43] Large-scale disclosure of this information can also occur online, as witnessed by the Julian Assange and Edward Snowden leaks.[44]

In part due to the ease with which information can now be gathered and disseminated, the focus of today's espionage is not limited to military or scientific secrets as occurred during the twentieth-century wars,[45] but has expanded to include political,[46] diplomatic,[47] economic,[48] corporate,[49] industrial,[50]

---

42 Matthew Castel, 'International and Canadian Law Rules Applicable to Cyber Attacks by State and Non-State Actors' (2012) 10 *Canadian Journal of Law and Technology* 89, 89; Pun (n 2) 355–6; see Mohanty (n 41).

43 Pun (n 2) 357–8, 379; Jupillat (n 26) 976; PJCIS (n 41) 3; Evidence to PJCIS, Parliament of Australia, Melbourne, 16 March 2018, 33 (Duncan Lewis, Director-General of Security, ASIO); Mohanty (n 41) 52; Sulick (n 26) 273; ASIO, *Counter-Espionage* (n 17); ASIO, *ASIO Annual Report 2017–18* (n 41) 25.

44 See, eg, Michael Scherer, 'The Geeks Who Leak' (24 June 2013) *Time Magazine*.

45 Of course, military and scientific information are still targeted today. See ASIO, *ASIO Annual Report 2016–17* (2017) 4, 24; ASIO, *ASIO Annual Report 2017–18* (n 41) 3; Evidence to PJCIS, Parliament of Australia, Canberra, 31 January 2018, 18 (Peter Vickery, Deputy Director-General, Counter-Espionage and Interference Capabilities, ASIO).

46 Evidence to PJCIS, Parliament of Australia, Canberra, 31 January 2018, 18 (Peter Vickery, Deputy Director-General, Counter-Espionage and Interference Capabilities, ASIO); ASIO, *ASIO Annual Report 2016–17* (n 45) 4; ASIO, ASIO, *ASIO Annual Report 2017–18* (n 41) 3; Castel (n 42) 89; Mohanty (n 41) 51.

47 Evidence to PJCIS, Parliament of Australia, Canberra, 31 January 2018, 18 (Peter Vickery, Deputy Director-General, Counter-Espionage and Interference Capabilities, ASIO); PJCIS (n 41) 2; ASIO, *ASIO Annual Report 2016–17* (n 45) 4; ASIO, *ASIO Annual Report 2017–18* (n 41) 3.

48 ASIO, *ASIO Annual Report 2016–17* (n 45) 4; ASIO, *ASIO Annual Report 2017–18* (n 41) 3; ASIO, Submission No 5 to PJCIS, *Review of Administration and Expenditure No 16 (2016–17)* 4; PJCIS (n 41) 2; Mohanty (n 41) 51; Kim (n 32) 753; Jupillat (n 26) 953; Banks (n 39) 513–14; Mark Klaver and Michael Trebilcock, 'Chinese Investment in the United States and Canada' (2013) 54 *Canadian Business Law Journal* 123, 130; Xingan Li, 'The Criminal Phenomenon on the Internet: Hallmarks of Criminals and Victims Revisited through Typical Cases Prosecuted' (2008) 5 *University of Ottawa Law and Technology Journal* 125, 134.

49 ASIO, *ASIO Annual Report 2016–17* (n 45) 4; ASIO, *ASIO Annual Report 2017–18* (n 41) 3; ASIO, Submission No 5 to PJCIS (n 48) 4; Banks (n 39) 513–14; see Lewis (n 26); Mohanty (n 41) 52.

50 ASIO, *ASIO Annual Report 2016–17* (n 45) 4; ASIO, *ASIO Annual Report 2017–18* (n 41) 3; ASIO, Submission No 5 to PJCIS (n 48) 4; Emir Crowne and Tasha De Freita, 'Canada's Inadequate Legal Protection Against Industrial Espionage' (2013) 13 *Chicago-Kent Journal of Intellectual Property* 192, 193.

technological,[51] intellectual property,[52] critical infrastructure[53] and natural resource information,[54] as well as physical items such as chemical substances or technology.[55] This information is now collected not just by 'enemy' nations, but also by any foreign government or organisation.[56] Where human intelligence officers are used, covers include students, scientists, businessmen and 'immigrants' seeking to resettle in Australia who target, for example, politicians, defence force personnel, journalists, academics and students.[57] Such espionage against Australia has long-term consequences, as it threatens to undermine national security, sovereignty and open democracy, and detrimentally impacts upon the country's national interests.[58]

In its 2016–17 Annual Report, the Australian Security Intelligence Organisation ('ASIO') stated that the current espionage threat against Australia was 'unprecedented'.[59] Then Prime Minister Malcolm Turnbull claimed that the

---

51 ASIO, *ASIO Annual Report 2016–17* (n 45) 4; ASIO, *ASIO Annual Report 2017–18* (n 41) 3; Evidence to PJCIS, Parliament of Australia, Canberra, 31 January 2018, 18 (Peter Vickery, Deputy Director-General, Counter-Espionage and Interference Capabilities, ASIO); PJCIS (n 41) 2; Mohanty (n 41) 52; Lewis (n 26) 192; Castel (n 42) 105.

52 ASIO, *ASIO Annual Report 2016–17* (n 45) 23; ASIO, Submission No 5 to PJCIS (n 48) 4; Banks (n 39) 513; Brian Johnson, Christopher Kierkus and Shannon Barton, 'The Economic Espionage Act and Trade Secret Theft: The Insider Threat' (2017) *Intellectual Property Quarterly* 152, 152; Mohanty (n 41) 52.

53 ASIO, *ASIO Annual Report 2016–17* (n 45) 24; ASIO, *ASIO Annual Report 2017–18* (n 41) 25.

54 ASIO, *ASIO Annual Report 2016–17* (n 45) 24; ASIO, *ASIO Annual Report 2017–18* (n 41) 25; Evidence to PJCIS, Parliament of Australia, Canberra, 31 January 2018, 18 (Peter Vickery, Deputy Director-General, Counter-Espionage and Interference Capabilities, ASIO); PJCIS (n 41) 2.

55 Jupillat (n 18) 951–2; *United States v Xiodong Sheldon Meng*: see US Department of Justice, *Chinese National Sentenced for Economic Espionage* (18 June 2008) <https://www.justice.gov/archive/opa/pr/2008/June/08-nsd-545.html>; Clive Hamilton, *Silent Invasion: China's Influence in Australia* (Hardie Grant, 2018) 152–3, 169, 171. For additional case examples, see William Hannas, James Mulvenon and Anna Puglisi, *Chinese Industrial Espionage: Technological Acquisition and Military Modernisation* (Routeledge, 2013) 256–70.

56 Evidence to PJCIS, Parliament of Australia, Canberra, 31 January 2018, 18 (Peter Vickery, Deputy Director-General, Counter-Espionage and Interference Capabilities, ASIO); Evidence to PJCIS, Parliament of Australia, Melbourne, 16 March 2018, 33 (Duncan Lewis, Director-General of Security, ASIO); PJCIS (n 41) 2–3; Jupillat (n 18) 953; ASIO, *Counter-Espionage* (n 17).

57 Kim (n 32) 752, 760; Lewis (n 26) 189, 206–7; Vara (n 30) 66; US Senate Intelligence Committee, Global Threats and National Security, C-SPAN, at 1:06.59-1:08.30 (13 February 2018) <https://www.c-span.org/video/?440888-1/fbi-director-rob-porter-background-check-completed-july&start=4136>; see Senate Select Committee on Intelligence, Parliament of the United States, *Open Hearing on Worldwide Threats* (2018) Senator Marco Rubio; Sulick (n 26) 265–74; Hamilton (n 55) 161–2, 179–82.

58 PJCIS (n 41) 2; Evidence to PJCIS, Parliament of Australia, Canberra, 31 January 2018, 18 (Peter Vickery, Deputy Director-General, Counter-Espionage and Interference Capabilities, ASIO); ASIO, *ASIO Annual Report 2017–18* (n 41) 3, 28; Commonwealth, *Parliamentary Debates*, House of Representatives, 7 December 2017, 13147 (Malcolm Turnbull).

59 ASIO, *ASIO Annual Report 2016–17* (n 45) 54; Revised Explanatory Memorandum, National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (Cth).

threat faced in 2017 was greater than the Soviet infiltration of the Australian Federal Government during World War II and the Cold War.[60] He highlighted threats to originate from the People's Republic of China ('PRC'), Russia, Iran and North Korea, all of which employ the espionage practices just described.[61]

Media reports suggest that most recent instances of actual, attempted or suspected espionage against Australia have been by the PRC. For example, Chinese telecommunications giant Huawei has been excluded from participating in Australia's 5G network amid concerns it would pose a national security risk, as the company is legally obliged to assist the Chinese government with 'state intelligence work'.[62] The Australian mining, metals and petroleum company BHP was warned by British Secret Intelligence that it was being spied on by China during its takeover bid of Rio Tinto in 2008.[63] Other examples include a Chinese hacking group's spreading of malware through cloud services used by Australian companies,[64] and Chinese theft of intellectual property and trade secrets from Australian universities and companies.[65] Concerns have also been raised over academic research collaborations between Australian scholars and Chinese research institutes that are linked to the Chinese Communist Party ('CCP') in regard to technology that could be used for military purposes.[66] Other instances

---

60 Commonwealth, *Parliamentary Debates*, House of Representatives, 7 December 2017, 13147 (Malcolm Turnbull).

61 Ibid 13146 (Malcolm Turnbull). See also Lewis (n 26) 191.

62 Michael Walsh and Ning Pan, 'What's next for Chinese tech giant Huawei after being banned from Australia's 5G network?', *ABC News* (online), 25 August 2018 <http://www.abc.net.au/news/2018-08-25/whats-next-for-huawei-after-being-banned-from-australias-5g/10160842>; Samantha Hoffman and Elsa Kania, 'Huawei and the ambiguity of Chinese intelligence and counter-espionage laws', *The Strategist* (online), 13 September 2018 <https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/>; see also Bethany Allen-Ebrahimian, 'Huawei, China's Shadowy Telecom Giant, Wants a Foothold in Europe', *The Daily Beast* (online), 1 August 2018 <https://search-proquest-com.ezproxy.library.uq.edu.au/docview/2081180279?rfr_id=info%3Axri%2Fsid%3Aprimo>; Hamilton, above n 51, 154–61; Rob Taylor and Sara Germano, 'At a Gathering of Spy Chiefs, US, Allies Agreed to Contain Huawei; Concerns are Shared by Top Intelligence Leaders from "Five Eyes" Intelligence-Sharing Network', *Wall Street Journal* (online), 14 December 2018 <https://search-proquest-com.ezproxy.library.uq.edu.au/docview/2157831507?accountid=14723>. See also Permanent Select Committee on Intelligence (House of Representatives), Parliament of the United States, *Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE* (2012) vi–vii.

63 Matthew Stevens, 'BHP was warned of tabs on deal', *The Australian Financial Review* (Melbourne), 27 July 2018, 32.

64 David Bond, 'Attackers spread malware through IT services providers', *Financial Times* (London), 12 July 2018, 1; see also Hamilton (n 55) 170, 176.

65 Andrew Tillett, 'Punish China cyber theft, urges ASPI', *The Australian Financial Review* (Melbourne), 25 September 2018, 10 ('*Punish China cyber theft*'); see also Hamilton (n 55) 169–70.

66 Lisa Murray and Andrew Tillett, 'Defence Power Grab Surprises', *The Australian Financial Review* (Melbourne), 18 July 2018, 5; Tillett, 'Punish China cyber theft' (n 65); Hamilton (n 55) 174, 176, 184–7, 190.

of espionage where it is unknown who was behind the conduct include data breaches at the Australian Commonwealth Scientific and Industrial Research Organisation ('CSIRO') facilities[67] and the hacking of a defence subcontractor where 30 gigabytes of secret data was stolen.[68]

Clive Hamilton, Professor of Public Ethics at Charles Sturt University, has argued that Australia is being actively targeted by the PRC for intelligence.[69] Although his arguments have attracted academic controversy and sparked critical discussions worldwide,[70] some of his claims are grounded in fact and provide an indication of the nature of Chinese espionage in Australia. For example, Confucius Institutes found in Australian universities and schools are publicly tasked with teaching Chinese language and culture, but Western intelligence agencies have identified them as a form of spy agency engaged in covert surveillance.[71] Furthermore, Chinese students and scholars' associations on university campuses tend to be funded by the CCP, and the CIA has described them as a system of student-informants engaged in political spying.[72]

III Australian Espionage Offences Before 2018

Australia's first espionage offence was modelled on s 1 of the United Kingdom's *Official Secrets Act 1911* and was introduced in 1914 with the *Crimes Act*. Section 78 of the *Crimes Act* consisted of just one offence where 'for any purpose prejudicial to the safety or interests of the Commonwealth' a person:

- approached or entered a prohibited place;
- made a sketch, plan, model or note that might or was intended to be useful to an enemy; or

---

67 Andrew Tillett, 'Overseas spy agencies 'target defence, industry'', *The Australian Financial Review* (Melbourne), 3 August 2018, 8; see Hamilton (n 55) 188–90.

68 Andrew Tillett, 'Overseas spy agencies 'target defence, industry'' (n 67).

69 Hamilton (n 55).

70 See, eg, Andrew Podger, *Book Review — Clive Hamilton's Silent Invasion: China's Influence in Australia* (21 March 2018) *The Conversation*, <https://theconversation.com/book-review-clive-hamiltons-silent-invasion-chinas-influence-in-australia-93650>; Rowan Callick, 'Clive Hamilton: Poking the Chinese Dragon', *The Australian* (online), 21 February 2018 <https://www.theaustralian.com.au/news/inquirer/clive-hamilton-poking-the-chinese-dragon/news-story/eef6add51ca1e0919236984b7f0b96be>; Rory Medcalf, 'Silent Invasion: The Question of Race', *The Interpeter* (online), 21 March 2018 < https://www.lowyinstitute.org/the-interpreter/silent-invasion-question-race>.

71 Hamilton (n 55) 217–18.

72 Ibid 225.

- obtained or communicated to any other person a sketch, plan, model or note or other document or information that might or was intended to be useful to an enemy.[73]

It was not necessary to show that the accused was guilty of any 'act tending to show a prejudicial purpose', but it was sufficient if such a purpose appeared from the 'circumstances of the case' or the accused's 'conduct or known character'.[74] Such a purpose was also presumed where the accused did not act under lawful authority.[75] The prescribed penalty was seven years' imprisonment.[76]

This offence was repealed in 2002 and replaced with four new offences[77] found in s 91.1 of the *Criminal Code*, each prescribing a maximum penalty of 25 years' imprisonment.[78] The rationale for the introduction of these new offences was to 'better deter and punish those who intended to betray Australia's security interests' and to reflect the 'modern intelligence environment'.[79] Each of the 2002 offences involved information concerning either the Commonwealth's security or defence, or the security or defence of another country where it was acquired from the Commonwealth.[80] 'Security or defence' was defined to include 'the operations, capabilities and technologies of, and methods and sources used by, a country's intelligence or security agencies'.[81]

The 2002 offences consisted of two offences of communicating or making available such information where it did or was likely to be communicated or made available to another country or foreign organisation.[82] It also consisted of two offences of making, obtaining or copying a record of such information intending that the record would or might be delivered to another country or foreign organisation.[83] Both types of conduct were criminalised where the person intended either to:

- prejudice the Commonwealth's security or defence;[84] or

---

73 *Crimes Act* s 78(1), as repealed by the *Espionage and Related Matters Act* sch 1 item 1.
74 Ibid s 78(2), as repealed by *Espionage and Related Matters Act* sch 1 item 1.
75 Ibid.
76 Ibid s 78(1), as repealed by *Espionage and Related Matters Act* sch 1 item 1.
77 See *Espionage and Related Matters Act* sch 1 items 1, 5.
78 *Criminal Code* s 91.1, as repealed by *Espionage Act* sch 1 item 17.
79 Revised Explanatory Memorandum, Criminal Code Amendment (Espionage and Related Matters) Bill 2002 (Cth) 1, 5.
80 *Criminal Code* s 91.1, as repealed by *Espionage Act* sch 1 item 17.
81 Ibid s 90.1(1) (definition of 'security or defence'), as repealed by *Espionage Act* sch 1 item 13.
82 Ibid s 91.1(1) and (2), as repealed by *Espionage Act* sch 1 item 17.
83 Ibid s 91.1(3) and (4), as repealed by *Espionage Act* sch 1 item 17.
84 Ibid s 91.1(1) and (3), as repealed by *Espionage Act* sch 1 item 17.

- advantage another country's security or defence, without lawful authority.[85]

A defence existed where the information was already communicated to the public with the Commonwealth's authority.[86] These offences applied to conduct that occurred both within and outside Australia.[87]

A *The Original and 2002 Offences Compared*

Before examining the 2018 offences, it is useful to first examine whether the 2002 offences effectively addressed espionage used today. By comparing the 2002 offences with the original offence, we can determine whether the 2002 offences better captured today's espionage practices, deterred espionage activity and supported convictions. We can then determine whether the 2018 offences were necessary. If the 2002 offences effectively achieved those ends, then it is possible that the 2018 offences were not actually needed.

1 *The Fault Element*

The original espionage offence criminalised conduct intended to prejudice the safety or interests of the Commonwealth. 'Prejudice' was not defined in the *Crimes Act* and has not been judicially considered, but the *Oxford English Dictionary* states it to mean 'harm or injury'.[88] However, this is a narrow definition, and in the context of the provision as a whole it was more likely to mean disadvantage or detriment.[89] 'Safety' was also not defined in the Act and has not been judicially considered; however, it is defined in the dictionary to mean protection from danger, risk or injury.[90] The original offence therefore appeared to target espionage that was intended to disadvantage the Commonwealth's ability to protect its people and borders from dangerous or injurious conduct. This choice of words reflected notions of wartime espionage where, for example, secrets were stolen to benefit the 'enemy' and therefore harm Australia during combat.

'Interests' was also not defined in the Act and has not been considered by the courts, making it unclear which specific Commonwealth interests the offence protected. The term may have included, for example, military, national security, economic, political or diplomatic interests. However, the Federal Parliament in its

---

85 Ibid s 91.1(2) and (4), as repealed by *Espionage Act* sch 1 item 17.
86 Ibid s 91.2, as repealed by *Espionage Act* sch 1 item 17.
87 Ibid s 91.1(7), as repealed by *Espionage Act* sch 1 item 17.
88 *Oxford English Dictionary* (n 1) 'prejudice'.
89 *Oxford English Thesaurus* (online ed at 21 June 2019) 'prejudice'.
90 *Oxford English Dictionary* (n 1) 'safety'.

Bills Digest for the Espionage and Related Matters Bill 2002 referred to the original offence as protecting 'traditional defence matters'.[91] It is likely that 'interests' was therefore intended to refer to the military and national security interests of the country. This was further indicated by the use of the combat-oriented word 'enemy' when referring to the one to whom the information might be useful.

In contrast, the 2002 offences criminalised conduct intended to 'prejudice the Commonwealth's security or defence' or 'give advantage to another country's security or defence'. Like the original offence, 'prejudice' was not defined in the *Criminal Code* and has not been judicially considered. Despite this, important changes were made. Instead of being limited to the Commonwealth's safety and interests alone, the 2002 offences appeared to broaden the fault element of the offence. It did this by including conduct intended to disadvantage Australia's security or defence generally, either by prejudicing Australia or by advantaging another country.

'Security or defence' was defined in the *Criminal Code* to include the 'operations, capabilities and technologies of, and methods and sources used by, the country's intelligence or security agencies'.[92] This definition narrowed the scope of 'security or defence' by indicating that it was the activities of a country's intelligence or security agencies alone that had to be prejudiced or advantaged. While it would still have captured theft of military, technological or diplomatic secrets, it is unclear whether the offences would have been sufficient to capture instances of espionage that, for example, intended to prejudice Australia's economic development, natural resource management strategies or vital infrastructure planning, or the trade secrets of Australian businesses, all of which are targeted by espionage today and can be used to compromise the country's national interests.[93] As such, the 2002 offences were too narrow to effectively address espionage practices used today.

2 *The Form of the Information*

The original sub-ss (b) and (c) of s 78 of the *Crimes Act* criminalised espionage relating to sketches, plans, models and notes. This limited the form of information that could be the subject of espionage and did not include, for

---

91 Parliament of Australia, *Bills Digest*, No 117 of 2001–2, 13 March 2002; see *Acts Interpretation Act 1901* (Cth) s 15AB regarding use of extrinsic materials in statutory interpretation.

92 *Criminal Code* s 90.1(1) (definition of 'security or defence'), as repealed by *Espionage Act* sch 1 item 13.

93 See, eg, ASIO, *ASIO Annual Report 2016–17* (n 45) 4, 23–4; ASIO, *ASIO Annual Report 2017–18* (n 41) 3, 25; ASIO, Submission No 5 to PJCIS (n 48) 4; Evidence to PJCIS, Parliament of Australia, Canberra, 31 January 2018, 18 (Peter Vickery, Deputy Director-General, Counter-Espionage and Interference Capabilities, ASIO). See also PJCIS (n 41) 1–5.

example, photographs, digital copies or electronic data that can now be collected due to advances in technology. Section 78(c) referred additionally to 'other documents or information'.[94] While this could have been construed broadly to include new forms of information targeted by espionage today, it only applied to obtaining or communicating such information and not other conduct that could be just as harmful to national security (for example, altering or copying the documents or information). Moreover, all forms of information were limited by the requirement that they 'might be or were intended to be directly or indirectly useful to an enemy'. Again, this reflected wartime espionage practices and not today's espionage environment where any foreign country can conduct espionage, not just 'enemies'.

The 2002 offences, however, referred to 'information', which was defined to mean 'information of any kind, whether true or false and whether in a material form or not, and includes an opinion, and a report of a conversation'.[95] This was a far broader definition than the form of information referred to in the original offence and would have captured photographs, digital copies or electronic data. However, it would still have failed to capture, for example, the physical theft, by a foreign country, of a newly developed chemical substance, type of material or item of technology to be analysed and produced for that foreign country.

Furthermore, the form of information was limited by the requirement that it concern 'the Commonwealth's security or defence' or 'the security or defence of another country, being information acquired directly or indirectly from the Commonwealth'.[96] The scope of 'security and defence' has been discussed above and meant that the type of information was generally limited to classified information concerning the operations of a country's security or intelligence agencies.[97] However, espionage today frequently targets unclassified information that may not have an immediate connection to a security or intelligence agency's activities but which may still nevertheless detrimentally impact upon national interests, such as economic or natural resource information.[98] The 2002 offences were therefore not drawn sufficiently to capture many espionage practices used today.

3 *The Type of Conduct*

The original offence of espionage required the person to 'make, obtain or communicate' the above information. This was narrow and would not have

---

94 *Crimes Act* s 78(c), as repealed by *Espionage and Related Matters Act* sch 1 item 1.
95 *Criminal Code* s 90.1(1) (definition of 'information'), as repealed by *Espionage Act* sch 1 item 13.
96 Ibid s 91.1, as repealed by *Espionage Act* sch 1 item 17.
97 See above Part III(A)(1).
98 See above nn 48 and 54.

included, for example, photocopying, photographing or providing a password or encryption key to access digital data. The 2002 offences broadened the type of conduct captured to include all of these things by making it an offence to 'communicate or make available' or 'make, obtain or copy a record' of information.[99] 'Make available' was not defined in the *Criminal Code* but could have referred to providing access to the information by, for example, giving another person a password, code or digital or physical key. These changes shifted the focus of espionage from outdated wartime espionage practices to today's espionage where technological advances mean that information may be collected and disseminated in far more technologically sophisticated ways.

4 *Other Differences*

Reflecting, again, the movement away from wartime espionage practices to espionage practices used in today's world was the removal, in the 2002 offences, of reference to 'enemy'. Instead, the offences referred to 'another country or foreign organisation, or person acting on behalf of such a country or organisation'. Although 'another country or foreign organisation' was not defined in the *Criminal Code*, its plain meaning indicates it would have included any country other than the Australian Commonwealth, or any foreign organisation, including, for example, terrorist organisations, international political bodies or non-governmental organisations, not just Australia's 'enemies'. This better reflects today's intelligence environment where states are not pitted against states in a global war, but rather each nation (or foreign organisation) seeks to serve its own self-interests.[100]

Furthermore, unlike the original 1914 offence, the 2002 offences included a requirement that the information 'is or is likely to be communicated or made available to another country or foreign organisation'. This made the offences more difficult to establish because it had to be shown that the information actually would, or was likely to be, given to another country. Under the original offence, the person may have intended the information to be useful to an enemy, but it was not necessary to establish that such information was actually going to be (or was likely to be) communicated to that enemy.

Finally, the 2002 offences specifically included a provision stating that the offences applied to conduct that occured outside Australia.[101] This effectively captured cyber espionage where intelligence officers engage in espionage against Australia's security or defence from the safety of another country such as their own.

---

99 *Criminal Code* s 91.1, as repealed by *Espionage Act* sch 1 item 17.

100 ASIO, *Counter-Espionage* (n 17).

101 *Criminal Code* s 91.1(7), as repealed by *Espionage Act* sch 1 item 17.

B *Did the 2002 Offences Effectively Address Espionage Used in Today's World?*

The original espionage offence was insufficient to capture practical instances of espionage used today, such as cyber espionage. This was largely remedied by the 2002 offences, which broadened the scope of conduct constituting an espionage offence. Despite these updates, the 2002 offences still failed to effectively address some aspects of today's espionage practices, as some key terms and definitions were too narrow or not appropriate. These included the definition of 'security or defence' as well as the form of information targeted by espionage.

Whether the 2002 offences effectively addressed espionage used in today's world is not limited to their scope but also requires consideration of their deterrent effect and the frequency of convictions. Deterrence is more effective where punishments are more certain and appropriately severe (for example, prescribed penalties of 25 years' imprisonment for the 2002 espionage offences).[102] Since the introduction of the original offence in 1914, there has only been one recorded case in which the accused was convicted of espionage.[103] This was under s 78 of the *Crimes Act* and has been described as the 'only major espionage trial in Australian jurisprudence'.[104] It is unknown whether others have been charged with espionage and pleaded guilty (hence their cases are not recorded), or have been brought to trial but acquitted.[105] Clive Hamilton claims that the lack of convictions for espionage in Australia is because 'there is no appetite' for prosecuting spies.[106] One explanation for the dearth of prosecutions could be Australia's 'catch and deport' system, where those suspected of spying have traditionally been deported instead of prosecuted under espionage laws.[107] Similarly, persons who have been considered espionage threats may simply have

---

102 Tim Newburn, *Criminology* (Routledge, 3rd ed, 2017) 552.

103 *R v Lappas* [2003] ACTCA 21.

104 Australian Law Reform Commission ('ALRC'), *Keeping Secrets Report: The Protection of Classified and Security Sensitive Information* (Report No 98, 2004) 38.

105 There appears to be no data on the frequency of espionage prosecutions in Australia, although former Prime Minister Malcolm Turnbull was quoted earlier in this article as saying that these espionage offences 'have not supported a single conviction in decades': Commonwealth, *Parliamentary Debates*, House of Representatives, 7 December 2017, 13148 (Malcolm Turnbull). This suggests that even if offenders have been prosecuted, their trials have not succeeded.

106 Hamilton (n 55) 162, 170.

107 Nick McKenzie, 'Agencies Step up Spy Hunt', *The Age* (online), 30 January 2018 <https://global-factiva-com.ezproxy.library.uq.edu.au/ga/default.aspx>; see, eg, Gordon Rayner, 'Theresa May Tells Vladimir Putin his Spy Network is Crippled after Allies Back Britain in Wake of Salisbury', *The Telegraph* (online), 27 March 2018 <https://www.telegraph.co.uk/news/2018/03/26/donald-trump-expels-60-russian-diplomats-response-salisbury/>.

had their visa applications refused.[108] This could reflect a desire by the Australian government not to prosecute on the basis that to do so would require disclosure of security sensitive or classified information, which would ultimately cause more harm to the country's national interests.[109] It has even been suggested that this 'anti-disclosure' stance may have been used by offenders to force the government to withdraw or reduce charges or enter into plea bargains.[110] While these administrative mechanisms may historically have provided some means of dealing with espionage in Australia, they would not be effective at addressing modern cyber espionage where information can be gathered from outside Australia.

Regardless of the reasons why only one espionage case has been recorded in Australian jurisprudence, espionage *is* occurring within and against Australia.[111] In its 2017–18 Annual Report, ASIO stated that it published 1440 intelligence reports covering terrorism, espionage and foreign interference threats against Australia and provided 245 assessments on the potential for foreign powers to conduct espionage, foreign interference or sabotage in Australia.[112] Numerous instances of espionage have also been reported in the media over the past year alone.[113] The 2002 offences therefore appear to have neither effectively deterred others from engaging in espionage nor supported effective prosecutions, despite their broadened scope.

---

108 ALRC (n 104) 9; see, eg, ASIO, Commonwealth of Australia, *Report to Parliament 1995–96* (1996) 95; ASIO, Commonwealth of Australia, *Report to Parliament 1996–97* (1997) 87. Other ASIO Annual Reports can be accessed at ASIO, *Previous Reports to Parliament* (2018) <https://www.asio.gov.au/previous-reports-parliament.html>.

109 ALRC (n 104) 10.

110 Ibid 10.

111 Hamilton (n 55) 181.

112 ASIO, *ASIO Annual Report 2017–18* (n 41) 39.

113 See above Part II(B).

IV The 2018 Espionage Offences

The *Espionage Act* repealed the four 2002 espionage offences and replaced them with 27 new offences.[114] Penalties are tiered and increase with the seriousness of the conduct, ranging from 15 years' imprisonment to life imprisonment. All offences apply to conduct within and outside Australia.[115]

The rationale for the introduction of the new offences was that the 2002 offences were too narrow and had failed to evolve with the modern threat environment.[116] While introducing the Espionage Bill in 2017, then Prime Minister Malcolm Turnbull stated that ASIO had issued 'very grave warnings' as to the threat of espionage, but that 'our agencies lacked the legislative tools they needed to act'.[117] He emphasised that 'our espionage laws are so unwieldy that they have not supported a single conviction in decades, even as the threat reaches unprecedented levels'.[118] He also stated that the new 'counter-foreign-interference strategy'[119] was built upon four pillars, one of which was deterrence.[120] These remarks highlight issues with the 2002 offences identified above, namely, their unsuitability to capture all aspects of espionage practices used in today's world, failure to deter offenders, and inability to support convictions.

---

114 See *Espionage Act* sch 1 item 17.

115 *Criminal Code* ss 91.7, 91.10, 91.14.

116 Revised Explanatory Memorandum, National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (Cth) 43 [16].

117 Commonwealth, *Parliamentary Debates*, House of Representatives, 7 December 2017, 13145 (Malcolm Turnbull).

118 Ibid 13148.

119 Ibid 13145.

120 Ibid.

A *Overview of the 2018 Offences*

Table 1: Overview of Underlying Espionage Offences

Offence	Section	Maximum Penalty
Espionage — dealing with security classified or national security information to be communicated to a foreign principal:		
(i) Intending to prejudice Australia's national security or advantage the national security of a foreign country	91.1(1)	Life
(ii) Reckless as to this prejudice or advantage	91.1(2)	25 years
Espionage — dealing with information to be communicated to a foreign principal:		
(i) Intending to prejudice Australia's national security	91.2(1)	25 years
(ii) Reckless as to this prejudice	91.2(2)	20 years
Espionage — dealing with security classified information to be communicated to a foreign principal:	91.3	20 years
'Espionage on behalf of a foreign principal'		
(i) Intending to prejudice Australia's national security or advantage the national security of a foreign country	91.8(1)	25 years
(ii) Reckless as to this prejudice or advantage	91.8(2)	20 years
(iii) No fault element as to this prejudice or advantage	91.8(3)	15 years
'Espionage-related offences'		
(i) Soliciting or procuring an espionage offence	91.11	15 years
(ii) Preparing or planning for an espionage offence	91.12	15 years
'Theft of trade secrets involving foreign government principal'	92A.1	15 years

The 27 new espionage offences consist of 11 underlying offences and 16 aggravated offences. Table 1 above provides an outline of the underlying offences, each of which will now briefly be discussed before turning to examine selected offences in greater detail.

The 2002 offences included two offences for communicating or making available security or defence information. These differed in their fault element: intention either to prejudice the Commonwealth's security or defence, or to advantage another country's security or defence. There were also two offences of making, obtaining or copying a record of such information that similarly differed in their fault element. The s 91.1(1) offence essentially combines these four offences into a single offence of dealing with national security or security classified information where the person either intended to prejudice Australia's national security or advantage the national security of a foreign country. Therefore, we will call it the 'core espionage offence'.

The s 91.1(2) offence differs from the core offence only in its fault element (recklessness instead of intention) and prescribed penalty (25 years' imprisonment instead of life imprisonment). Contrary to most serious criminal offences that have a fault element of 'intention', 'recklessness' renders a person's conduct criminal where that person has a much lower level of personal culpability. This is because all that must be shown is that the person was aware of a substantial risk that a circumstance existed or a result would occur and it was unjustifiable for them to take that risk in the circumstances.[121] This could capture the conduct of people who merely failed to comprehensively investigate what they were doing or where, for example, an ASIO officer accidentally left a work laptop on a train.[122] Concerns regarding the scope of this fault element in its application to such a serious offence naturally arise.

The two s 91.2 offences differ from each other only in their fault element and prescribed penalties (25 years' imprisonment for intention and 20 years' imprisonment for recklessness).[123] They criminalise dealing with any information, whether true or false,[124] so long as the person has the intention to,[125] or is reckless that,[126] their conduct will prejudice Australia's national security. It is not necessary that the information actually concern Australia's national security. While this means that people could face severe punishment where their conduct has not actually disadvantaged national security interests, the offence

---

121 *Criminal Code* s 5.4.

122 Andrew Lynch, George Williams and Nicola McGarrity, *Inside Australia's Anti-Terrorism Laws and Trials* (NewSouth, 2015) 36–7.

123 *Criminal Code* ss 91.2(1) and (2).

124 Ibid s 90.1(1) (definition of 'information').

125 Ibid s 91.2(1).

126 Ibid s 91.2(2).

will likely prove useful in sting-operation scenarios where law enforcement suspects that a person is engaging in espionage and sets them up with 'bait' information to confirm their criminal activities. It is arguable, though, that even this is an overreaching of the law.

Section 91.3 of the *Criminal Code* contains a single offence for dealing with security classified information with the primary purpose of communicating it to a foreign principal or person acting on its behalf. The prescribed penalty is 20 years' imprisonment.[127] This offence targets traditional espionage activities and shares some of the core offence's key terms and elements.

The next three underlying offences are found in s 91.8 and criminalise engaging in espionage on behalf of a foreign principal. The three offences again differ only in their fault element (intention, recklessness or no mental element in regard to prejudicing Australia's national security or advantaging the national security of a foreign country) and prescribed penalties (25, 20 and 15 years' imprisonment, respectively).[128] While the relevant fault elements raise concerns regarding the scope of the offences, as with the s 91.3 offence these three offences fall within traditional espionage. They also share some key terms and elements with the core offence.

In addition to the abovementioned offences, two 'espionage-related offences' were also introduced by the *Espionage Act*.[129] Section 91.11 of the *Criminal Code* now makes it an offence to solicit or procure an espionage offence.[130] It carries a prescribed penalty of 15 years' imprisonment.[131] For the first time, this offence targets the conduct of recruiters and not the intelligence officers themselves, and it does not require commission of an actual espionage offence. The second espionage-related offence is found in s 91.12 and criminalises preparing for or planning an espionage offence. It also carries a prescribed penalty of 15 years' imprisonment.[132] This is the most extreme of the 2018 offences and resembles the 'catch-all'[133] preparatory terrorism offence[134] over which many concerns have been raised.

The final underlying offence criminalises the dishonest theft of trade secrets either on behalf of or where directed, funded or supervised by a foreign government principal.[135] The prescribed penalty is 15 years' imprisonment. While not strictly an espionage offence, this offence still effectively captures instances

127 Ibid s 91.3(1).
128 Ibid ss 91.8(1), (2) and (3).
129 Ibid sub-div C.
130 Ibid s 91.11(1).
131 Ibid.
132 Ibid s 91.12(1).
133 Lynch, Williams and McGarrity (n 122) 29.
134 See *Criminal Code* s 101.6.
135 Ibid s 92A.1(1).

of commercial and trade-related espionage conducted on behalf of a foreign government principal.

Aside from these underlying offences, 16 aggravated offences were also introduced by the 2018 Act. Where an offence is found to be aggravated, the prescribed penalty is increased either to life imprisonment (from 25 years' imprisonment), or to 25 years' imprisonment (from 20 years' imprisonment).[136] Aggravating circumstances are:

- 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
- holding an Australian Government security clearance allowing access to at least 'secret' security classified information, at the time the person dealt with the information.[137]

While there are only four aggravating circumstances, they each apply to the ss 91.1(2),[138] 91.2(1),[139] 91.2(2)[140] and 91.3(1)[141] offences.[142] This effectively creates a novel scheme of 16 aggravated offences that increase the maximum penalty available in circumstances where espionage is generally considered to be more serious.

Three defences are available to a charged espionage offence. The first arises where the person dealt with information according to a Commonwealth law or in their capacity as a public official.[143] The second arises where the information was already communicated to the public with the Commonwealth's authority.[144]

---

136 Ibid s 91.6(1).

137 Ibid.

138 Espionage — dealing with security classified or national security information to be communicated to a foreign principal, reckless as to prejudicing Australia's national security or advantaging the national security of a foreign country.

139 Espionage — dealing with information to be communicated to a foreign principal, intending to prejudice Australia's national security.

140 Espionage — dealing with information to be communicated to a foreign principal, reckless as to prejudicing Australia's national security.

141 Espionage — dealing with security classified information to be communicated to a foreign principal.

142 *Criminal Code* s 91.6(1).

143 Ibid s 91.4(1).

144 Ibid s 91.4(2).

These two defences apply to ss 91.1,[145] 91.2,[146] 91.3[147] and 91.8,[148] while the first alone applies to the two 'espionage-related offences'.[149] The third defence ('prior publication defence') applies to ss 91.1(1) and 91.1(2)[150] (where the prosecution relies on the fault element of intending to advantage the national security of a foreign country) as well as to s 91.3.[151] The following must be satisfied for the prior publication defence to arise: the person must not have made or obtained the information as a result of being a Commonwealth officer; the information must have already been communicated to the public; the person must not have been involved in the prior publication; the person must have believed that dealing with the information would not prejudice Australia's national security; and the person must have had reasonable grounds for that belief regarding the nature, extent and place of prior publication.[152]

Concerns arise over the scope and appropriateness of these defences, particularly regarding the adequacy of protections for investigative journalists, whistleblowers and the exercise of civil liberties.[153] Notably, there is no specific defence for 'news reporting', as was included with the 2018 amendments to Australia's secrecy offences.[154] This is of particular concern considering the Australian Federal Police raids on the home of News Corp journalist Annika Smethurst and the headquarters of ABC Sydney that occurred in June 2019.[155]

---

145 Espionage — dealing with security classified or national security information to be communicated to a foreign principal, intending to or reckless as to prejudicing Australia's national security or advantaging the national security of a foreign country.

146 Espionage — dealing with information to be communicated to a foreign principal, intending to or reckless as to prejudicing Australia's national security.

147 Espionage — dealing with security classified information to be communicated to a foreign principal.

148 'Espionage on behalf of a foreign principal'; *Criminal Code* ss 91.4, 91.9.

149 *Criminal Code* ss 91.11, 91.12, 91.13.

150 Espionage — dealing with security classified or national security information to be communicated to a foreign principal, intending to or reckless as to prejudicing Australia's national security or advantaging the national security of a foreign country.

151 Espionage — dealing with security classified information to be communicated to a foreign principal.

152 *Criminal Code* s 91.4(3).

153 See Australian Lawyers for Human Rights, Submission No 7 to PJCIS, Parliament of Australia, *Review of the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017*, 22 January 2018, 6; Whistleblowers Australia, Submission No 51 to PJCIS, Parliament of Australia, *Review of the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017*, 26 March 2018, 3–4, 7; Human Rights Watch, Submission No 10 to PJCIS, Parliament of Australia, *Review of the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017*, 22 January 2018; Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Human Rights Scrutiny Report* (2018) 246–54.

154 *Criminal Code* s 122.5(6).

155 Paul Karp, 'Federal Police Raid Home of News Corp Journalist Annika Smethurst', *The Guardian* (online, 4 June 2019) <https://www.theguardian.com/australia-news/2019/jun/04/federal-

Although these raids did not involve espionage offences, they were conducted on the basis of other national security offences that similarly do not provide much, if any, protection for journalists.[156] This article does not intend to analyse these lack of protections in further detail but merely seeks to highlight that they exist. It is recommended that an in-depth examination of the costs of the 2018 offences and their defences be conducted in the near future to allow for a more comprehensive assessment of the new offences.

To determine whether the 2018 espionage offences are necessary to effectively address espionage in today's world, the core, solicitation and preparatory offences will now be examined in detail. The core offence provides a foundation for examining differences in key terms and definitions between the 2002 and 2018 offences, which is useful to determine whether the 2018 offences will better address espionage practices used today. The solicitation and preparatory offences are novel and more extreme than the 2002 and other 2018 offences. They are of interest to determine whether the 2018 offences will meet deterrence aims and support convictions. The remaining offences, as well as the aggravating circumstances and defences, will not be examined in detail.

B *The Core Espionage Offence*

Section 91.1(1) of the *Criminal Code* combines the four 2002 offences into a single offence. However, it differs from the 2002 offences, as the prescribed penalty has been increased from 25 years' imprisonment to life imprisonment, and key terms and definitions have been altered.

The provision criminalises dealing with information or an article that either has a secret or top secret security classification or concerns Australia's national security where the person has the intention of:

- prejudicing Australia's national security; or

police-raid-home-of-news-corp-journalist-annika-smethurst>; Amy Remeikis, 'ABC Vows to Continue Reporting 'Without Fear' after Police Raid Sydney Offices' *The Guardian* (online, 5 June 2019) <https://www.theguardian.com/media/2019/jun/05/abc-offices-raided-by-australian-federal-police>.

156 Editorial, 'Balance National Security with Public Right to Know' *The Australian* (online, 7 June 2019) <https://www.theaustralian.com.au/commentary/editorials/balance-national-security-with-public-right-to-know/news-story/028f41ac640c75a3cae9e365832340 49>; Rebecca Ananian-Welsh, 'Why the Raids on Australian Media Present a Clear Threat to Democracy', *The Conversation* (online, 5 June 2019) <http://theconversation.com/why-the-raids-on-australian-media-present-a-clear-threat-to-democracy-118334>; Elise Worthington and Clare Blumer, 'What do the AFP Raids on the Media mean for Journalists and their Sources?' *ABC News* (online, 7 June 2019) <https://www.abc.net.au/news/2019-06-06/abc-raids-what-they-tell-us-about-press-freedom/11187364>.

- advantaging the national security of a foreign country.[157]

Additionally, the person's conduct must, or will, result in the information or article being communicated or made available to a foreign principal.[158]

1 *The Fault Element*

Problems with the limited definition of 'security or defence' in the 2002 offences have been remedied by the s 91.1(1) offence where the person must have acted with the intention of prejudicing 'Australia's national security' or advantaging the 'national security of a foreign country'. Unlike the 2002 offences, the *Criminal Code* specifies that 'embarrassment alone' is not sufficient to constitute 'prejudice',[159] which means that the offence cannot be used to silence those who may disseminate information that merely embarrasses the government (such as exposure of a blunder or mistake made by the Australian government). However, 'prejudice' has not been defined further. The *Criminal Code* does define 'national security' to mean defence of the country, protection of its borders from serious threats, and protection of the country and its people from activities such as espionage, terrorism, foreign interference and conduct obstructing operations of the country's defence force.[160] More broadly, it also includes the 'carrying out of the country's responsibilities to any other country' and the country's 'political, military or economic relations with another country'.[161]

This broad definition of 'national security' significantly expands the fault element of the offence beyond the scope of the 2002 offences. It potentially criminalises conduct intending to prejudice almost any aspect of Australia's national security and not just the activities of intelligence or security agencies. This also applies to conduct intending to advantage the national security of a foreign country. This could include conduct intended to prejudice Australia's, or advantage another country's, economy (for example, by intentional manipulation of the stock market), natural resource management strategies, critical infrastructure plans, trade secrets, or breakthroughs in scientific research, all of which have the potential to detrimentally affect national interests.[162] Significantly, the definition explicitly refers to 'political or economic

---

157 *Criminal Code* s 91.1(1).
158 Ibid s 91.1(1).
159 Ibid s 90.1(1) (definition of 'prejudice').
160 Ibid ss 90.4(1)(a)–(c), 90.4(2).
161 Ibid s 90.4(1)(d) and (e).
162 Today's espionage frequently targets these things. See, eg, ASIO, *ASIO Annual Report 2016–17* (n 45) 4, 23–4; ASIO, *ASIO Annual Report 2017–18* (n 41) 3, 25; ASIO, Submission No 5 to PJCIS (n 48) 4; Evidence to PJCIS, Parliament of Australia, Canberra, 31 January 2018, 18 (Peter Vickery, Deputy

relations' with other countries, which recognises the major role that diplomatic and economic information plays in espionage today.[163] The 2002 offences were insufficiently broad to capture such information.

2 *The Form of Information*

The core espionage offence refers to 'information or an article'. 'Information' has the same definition as the 2002 offences: 'information of any kind, whether true or false and whether in a material form or not, and includes an opinion, and a report of a conversation'.[164] However, the core offence additionally refers to 'article', which includes 'any thing, substance or material'.[165] This is much broader than the 2002 offences and would include, for example, physical samples of a new chemical substance, type of material or piece of technology, not merely information about that item. Today's espionage can target such items.[166]

Similar to the 2002 offences, the form of information captured by the offence is limited, as it must 'have a security classification' (of secret or top secret)[167] or 'concern Australia's national security'. The security classification requirement covers information traditionally targeted by espionage, such as military or defence documents,[168] and so this is an appropriate qualification. The alternative requirement is less strict but still attempts to ensure that only information concerning national security, and not any information whatsoever, is the subject of criminal liability. However, as we have seen, the definition of 'national security' is quite broad, and so a vast array of information (or articles) could fall within the offence. For example, unclassified information regarding Australia's economic development, natural resources, political goals or trade policies could be captured, all of which could threaten national interests.[169] It is also possible that some information captured may not in reality harm Australia's national interests, raising concerns over the broad scope of the definition. For example, 'national security' has been defined to include the 'carrying out of the country's

---

Director-General, Counter-Espionage and Interference Capabilities, ASIO). See also PJCIS (n 41) 1–5.

163 *Criminal Code* ss 90.4(1)(d) and (e). See, eg, ASIO, *ASIO Annual Report 2016–17* (n 45) 4; ASIO, *ASIO Annual Report 2017–18* (n 41) 3; Evidence to PJCIS, Parliament of Australia, Canberra, 31 January 2018, 18 (Peter Vickery, Deputy Director-General, Counter-Espionage and Interference Capabilities, ASIO); Klaver and Trebilcock (n 48) 130; Mohanty (n 41) 51.

164 *Criminal Code* s 90.1(1) (definition of 'information').

165 Ibid s 90.1(1) (definition of 'article').

166 Jupillat (n 18) 951–2; *United States v Xiodong Sheldon Meng*: see US Department of Justice (n 55); Hamilton (n 55) 152–3, 169, 171. For additional case examples, see Hannas, Mulvenon and Puglisi (n 55) 256–70.

167 *Criminal Code* s 90.5.

168 Ibid.

169 See above n 162.

responsibilities to any other country'.[170] This could refer merely to Australia's aid obligations to other countries. Information concerning this topic is unlikely to prejudice national interests to the extent that criminal punishment is warranted.

3 *The Type of Conduct*

The s 91.1(1) offence refers to 'dealing with' the information or article. This includes dealing with all or part of the information or article, or dealing only with the 'substance, effect or description' of it.[171] Like the 2002 offences, 'deal with' is defined to include communicating, making available, making, obtaining or copying.[172] However, it adds to this by also including receiving, collecting, possessing, altering, concealing and publishing.[173]

The core offence further expands on the 2002 offences by defining 'make available'. This term means placing the information or article somewhere to be accessed by another, giving it to an intermediary to give to a recipient, or describing how to obtain access to it or methods that are likely to facilitate access to it.[174] This clarifies the meaning of 'make available' and would include, for example, describing where certain documents are located in a building or handing over a password or encryption key to access digital data.

4 *Other Differences*

The 2002 offences referred to 'another country or foreign organisation or person acting on its behalf', but 'foreign organisation' was not defined. The core offence, however, refers to a 'foreign principal or person acting on its behalf'. 'Foreign principal' has been defined to include a foreign government principal or political organisation, public international organisation, terrorist organisation or entity owned, directed or controlled by any of these foreign principals.[175] 'Foreign government principal' includes foreign governments (including local governments) or their authorities, foreign public enterprises, or entities owned, directed or controlled by a foreign government principal.[176]

These definitions provide more clarity than the 2002 provisions and also broaden the scope of to whom it is intended that the information be conveyed by including entities or organisations 'owned, directed or controlled' by a foreign

---

170 *Criminal Code* s 90.4(1)(d).
171 Ibid s 90.1(2)
172 Ibid s 90.1(1) (definition of 'deal').
173 Ibid.
174 Ibid (definition of 'make available').
175 Ibid s 90.2.
176 Ibid s 90.3.

principal. This could include, for example, Chinese student societies being run on university campuses that are funded and/or directed by the CCP and require their members to engage in espionage while in Australia.[177]

C *The Solicitation Offence*

Section 91.11(1) of the *Criminal Code* makes it an offence to engage in conduct with the 'intention of soliciting or procuring, or making it easier to solicit or procure', another person (the 'target') to deal with information in a way that would constitute an offence against Subdivision A (espionage) or Subdivision B (espionage on behalf of a foreign principal). In addition, the conduct must be engaged in on behalf of or in collaboration with a foreign principal or be directed, funded or supervised by a foreign principal.[178]

This offence focuses on the conduct of recruiters of spies and not the spies themselves; it is not necessary for the target to have actually committed an espionage offence or for such conduct to even be possible.[179] For example, the offence could capture foreign government ministers or businesspersons who attempt to bribe Australian government officials for information that could prejudice the national security of Australia or advantage another country's national security.[180] Furthermore, reference to 'making it easier' to solicit or procure an espionage offence could include, for example, merely befriending (or seducing) Australian government officials, lavishing gifts on them, providing free travel to the foreign country[181] or making political donations. Hamilton argues that these activities are all engaged in by the PRC, whose operatives use such tactics to obtain information pertaining to Australia's national security.[182]

The solicitation offence will likely be an effective deterrent, as it is the conduct of those procuring others to engage in espionage that is targeted, not the conduct of intelligence officers themselves. Despite the seriousness of such conduct, the prescribed penalty is merely 15 years' imprisonment, which is the lowest maximum penalty prescribed for the 2018 offences. To better deter potential foreign actors, the prescribed penalty could be more severe. Nevertheless, this offence will likely be easier to prosecute successfully, as it does not require the actual commission of an espionage offence or for such an offence to be possible. Additionally, 'making it easier' to solicit or procure an espionage

---

177 Clive Hamilton claims that this occurs. See Hamilton (n 55) 225. See also Lewis (n 26) 189.

178 *Criminal Code* s 91.11(1).

179 Ibid s 91.11(3).

180 This has occurred in the past. See Evidence to PJCIS, Parliament of Australia, Canberra, 31 January 2018, 21, 33–4 (Peter Vickery, Deputy Director-General, Counter-Espionage and Interference Capabilities, ASIO); Klaver and Trebilcock (n 48) 130.

181 This occurred in the Unites States: *United States v Gowadia*, 760 F 3d 989 (9th Cir, 2014).

182 Hamilton (n 55) 67–9, 73–8, 83–6, 95, 165.

offence can be construed broadly to include a vast range of conduct that could even appear to be innocent.

D *The Preparatory Offence*

Section 91.12(1) of the *Criminal Code* makes it an offence to engage in conduct with the 'intention of preparing for, or planning, an offence against Subdivision A (espionage) or Subdivision B (espionage on behalf of a foreign principal)'. The prescribed penalty is 15 years' imprisonment.

This offence resembles the catch-all 'preparing for or planning terrorist acts' offence found in s 101.6 of the *Criminal Code*, which prescribes a maximum penalty of life imprisonment. That offence was introduced after the September 11 terrorist attacks, along with a suite of other terrorism offences.[183] Concerns were immediately raised regarding the scope of the offence and the severity of the punishment,[184] as it was held that it 'distorted the traditional focus of the criminal law by punishing activities preliminary to the commission of a substantive offence'.[185] As the Independent National Security Legislation Monitor ('INSLM') described in its 2011 Annual Report:

> There need be no specific act in mind and the possibility of plural acts therefore comprehends a state of mind where a range of choices or possibilities exists without any decision to carry out one or more of them.[186]

INSLM highlighted that a person could contravene s 101.6 where they engage in a mundane activity, such as ascertaining a public transport timetable or merely think about committing a terrorist act.[187] These concerns have since been realised, with convictions achieved on the basis of, for example, possessing hunting

---

183 Keiran Hardy and George Williams, 'Australian Legal Responses to Foreign Fighters' (2016) 40 *Criminal Law Journal* 196, 198–9; The Hon Susan Kiefel AC, 'Judicial Decision-Making in Times of War and Relative Peace' (2018) 92 *Australian Law Journal* 708, 713; Charisse Smith and Mark Nolan, 'Post-Sentence Continued Detention of High-Risk Terrorist Offenders in Australia' (2016) 40 *Criminal Law Journal* 163, 163; Lynch, Williams and McGarrity (n 122) 26.

184 Council of Australian Governments ('COAG'), Commonwealth of Australia, *Council of Australian Governments Review of Counter-Terrorism Legislation* (2013) 13; Independent National Security Legislation Monitor ('INSLM'), Commonwealth of Australia, *Annual Report 16 December 2011* (2012) 50, 55; George Williams, 'The Legal Legacy of the 'War on Terror'' (2013) 12 *Macquarie Law Journal* 3, 5, 8.

185 Lynch, Williams and McGarrity (n 122) 31; INSLM (n 184) 55; Jude McCulloch, 'Human Rights and Terror Laws' (2015) 128 *Precedent* 26, 28.

186 INSLM (n 184) 55.

187 Ibid 55.

knives,[188] conducting reconnaissance of potential targets,[189] and purchasing boxes of screws that could potentially be used as shrapnel.[190]

Concerns were also raised over the application of the inchoate offences of attempt and conspiracy to the already broad preparatory offences.[191] A person attempts to commit an offence when they intend to engage in conduct constituting an offence or know that their conduct would constitute an offence,[192] but their conduct is more than merely preparatory.[193] It is possible to be found guilty of attempt even if commission of the offence is impossible or the person actually committed the attempted offence.[194] Conspiracy requires two or more people to agree to commit an offence and at least one of the conspirators engages in overt conduct in pursuance of the agreement.[195] Where found guilty of either offence, the offender is liable to the same punishment prescribed for the substantive offence.[196] These inchoate offences criminalise the very early stages of a possible criminal act where the person may not have even decided precisely what they intend to do.[197] Conspiracy in particular may arise where a crime has not been committed or even attempted, or where no evidence exists of a plan to commit a specific crime.[198]

Concerns over the offence of attempting to prepare for a terrorist attack have proved to be unfounded. Attempt requires the act to be more than preparatory, which is logically inconsistent with preparatory offences.[199] As such, the offence has never been used. The conspiracy offence, however, has been routinely relied upon in recent years[200] and has supported lengthy prison sentences of 22 and a

188 *R v HG* [2018] NSWSC 1849.
189 *R v Khaja [No 5]* [2018] NSWSC 238.
190 *DPP (Cth) v MHK (A Pseudonym)* [2017] VSCA 157.
191 INSLM (n 184) 58; Williams, 'Legal Legacy' (n 184) 8; Lynch, Williams and McGarrity (n 122) 32.
192 *Criminal Code* s 11.1.
193 Ibid s 11.1(2).
194 Ibid s 11.1(4).
195 Ibid s 11.5.
196 Ibid ss 11.1 and 11.5.
197 COAG (n 184) 12–13; INSLM (n 184) 58; McCulloch (n 185) 28; Lynch, Williams and McGarrity (n 122) 33; see, eg, *Lodhi v R* (2006) FLR 303, 318 and *R v Badya*; *R v Namoa [No 8]* [2019] NSWSC 24 ('*Badya and Namoa*').
198 Carmel O'Sullivan and Mark Lauchs, 'A Spoiled Mixture: The Excessive Favouring of Police Discretion over Clear Rules by Queensland's Consorting Laws' (2018) 42 *Criminal Law Journal* 108, 110; see *Badya and Namoa* (n 197).
199 Lynch, Williams and McGarrity (n 122) 33.
200 See, eg, *Badya and Namoa* (n 197); *R v Abbas* [2018] VSC 553 ('*Abbas*'); *R v Khalid* [2017] NSWSC 1365 ('*Khalid*'); *R v Al-Kutobi*; *R v Kiad* [2016] NSWSC 1760 ('*Al-Kutobi*'); INSLM (n 184) 58. See also Lynch, Williams and McGarrity (n 122) 35–8; Jessie Blackbourn and Nicola McGarrity, *Prosecutions* (8 Feb 2017) Australian National Security Law <https://ausnatsec.wordpress.com/prosecutions>.

half years,[201] 24 years[202] and 28 years.[203] Juveniles have even been convicted under the offence, with a 14-year-old receiving a sentence of 13 years' imprisonment for sourcing four weapons that he proposed should be used by his fellow conspirators in a terrorist attack.[204] While conduct found to be criminal included purchasing chemicals and items to make improvised explosive devices,[205] as well as conducting internet searches on how to make a bomb,[206] it extended so far as to include mere 'talk'.[207] For example, in *R v Khalid*,[208] those convicted had held meetings to discuss committing a terrorist act and exchanged crudely coded telephone messages on the subject.[209] In one case, two 18-year-old offenders were found guilty 'without having resolved upon a particular terrorist act'.[210]

These concerns of overreach apply equally to the new s 91.12 preparatory espionage offence, which is a similarly wide offence. Interestingly, the inchoate offence of attempt does not apply to the preparatory espionage offence,[211] thereby addressing the conceptual difficulties discussed above. However, the offence of conspiracy to prepare for an espionage offence can be relied upon by law enforcement. As with terrorism, such an offence drastically broadens the scope of conduct that is criminalised. For example, merely discussing with another person the best way to access classified documents, or asking about the various methods of encryption used by the defence force, is criminalised. The people involved may not ever carry out their plan or the plan may not yet be precisely defined, but this preliminary conduct would be sufficient to engage the offence of conspiracy to prepare for espionage.

These concerns are heightened when we further consider the broad scope of the preparatory offence itself. Preparing for or planning an espionage offence could include conduct that significantly falls short of any substantive espionage offence and may have an innocent explanation, such as purchasing a laptop (which could be used for cyber espionage) or phone (to take photographs of documents). Conspiracy would capture merely talking to another person about doing those things.

The conspiracy to prepare for a terrorist act offence was criticised for its severe punishment, as those found guilty are liable to the maximum penalty (life

---

201 *Khalid* (n 200).
202 *Abbas* (n 200).
203 *R v Elomar* [2010] NSWSC 10.
204 *Khalid* (n 200).
205 *Abbas* (n 200); *Al-Kutobi* (n 200).
206 *Abbas* (n 200).
207 Lynch, Williams and McGarrity (n 122) 39.
208 *Khalid* (n 200).
209 Ibid.
210 *Badya and Namoa* (n 197) [8].
211 *Criminal Code* s 91.12(2).

imprisonment) for the preparatory offence, despite not having engaged in any substantive terrorism offence.[212] The preparatory espionage offence appears to address these concerns by providing a maximum prescribed penalty of only 15 years' imprisonment.[213] However, this is still severe compared to the broad and apparently innocent conduct that can be captured by the offence.

If the similar terrorism offences provide an indication of how the 2018 espionage offences will be used, it is likely the conspiracy to prepare for an espionage offence will be the most frequently used of all the 2018 offences. The offence will be far easier to prove than the core espionage offence and will therefore likely result in a greater number of convictions; all the prosecution must establish is that the person communicated to someone else about doing something in preparation to commit espionage. More frequent convictions with the potential for still relatively severe prison sentences should act as a deterrent to better prevent the commission of espionage against Australia. However, the broad scope of this offence raises serious human rights concerns that have similarly been raised regarding the terrorism offences,[214] particularly regarding the over-criminalisation of conduct that could have an innocent explanation.[215] These concerns should be given more detailed consideration, but this is beyond the scope of this article.

V Are The 2018 Offences An Effective Tool Against Espionage Used in Today's World?

While the 2002 offences improved on the original 1914 offence to better address instances of espionage used today, they still failed to capture key aspects of today's espionage practices. They also failed to deter others from engaging in espionage and did not effectively support convictions. As such, it was necessary that Australia's espionage offences be amended to address these problems. These amendments took the form of the 2018 offences.

The 2018 offences have broadened the scope of espionage conduct captured by altering key terms and definitions that underpin the core espionage offence.

---

212 INSLM (n 184) 58; Williams, 'Legal Legacy' (n 184) 5; Lynch, Williams and McGarrity (n 122) 32.

213 *Criminal Code* s 91.12(1).

214 Hardy and Williams (n 183) 207–8; Justice François Kunc, 'Current Issues' (2017) 92 *Australian Law Journal* 255, 258; Tracy Albin, 'The Battle of Civil Liberties and the Vulnerability of Terrorism: How do we Avoid an Orwellian Society?' (2017) 2 *Perth International Law Journal* 12; Williams, 'Legal Legacy' (n 184) 6, 11–12.

215 COAG (n 184) 13; INSLM (n 184) 58; Williams, 'Legal Legacy' (n 184) 8, 14; Nicola McGarrity, '"Testing" our Counter-Terrorism Laws: The Prosecution of Individuals for Terrorism Offences in Australia' (2010) 34 *Criminal Law Journal* 92; George Williams, 'A Decade of Australian Anti-Terror Laws' (2011) 35 *Melbourne University Law Review* 1136; Lynch, Williams and McGarrity (n 122) ch 2.

These changes mean that the core offence, as well as other 2018 offences that share the key terms, will more effectively address espionage practices used in today's world than the 2002 offences. Their broad scope will also suffice to meet modern technological advances, making the offences adaptable to future changes in espionage practices. The solicitation and preparatory offences will likely prove effective at achieving more convictions and deterring others from committing espionage. As novel offences, not only is the conduct of recruiters now criminalised even where a substantive espionage offence has not been or cannot be committed,[216] but so too are mere preparatory acts[217] and conspiracies to engage in preparatory acts.[218] These offences will certainly be far easier to establish than the core offence, which will probably better support convictions. ASIO has stated that the new offences will provide 'valuable new tools to help combat [the espionage] threat [and] offer a significant public deterrent'.[219] Despite this, we cannot ignore their potential impact on human rights and the rule of law. Specifically, some of the offences capture a broad range of conduct at a very early stage. This conduct may even have an innocent explanation.

The core, solicitation and preparatory offences are therefore necessary to effectively address espionage used in today's world. They are sufficiently wide to capture today's espionage practices and will likely be sufficiently easy to prove, with relatively severe penalties to secure convictions and deter others. While these offences are necessary, it does not mean that the other 2018 offences are also necessary. Many of the other offences share the key underlying terms and definitions discussed in relation to the core offence. They also draw on aspects of that offence by selectively including some of its elements. However, not all elements are included, which makes many of the offences not discussed in detail less strict than the core offence. This means that certain conduct may fall within a number of the 2018 offences and may be easier to prove under one offence compared to another.

For example, s 91.3 of the *Criminal Code* criminalises dealing with security classified information to be communicated to a foreign principal where the person had the primary purpose of communicating the information to a foreign principal. Unlike the core offence, this offence concerns security classified information alone and not national security information as well. It is also not necessary to show that the person intended to prejudice Australia's national security or advantage the national security of another country. As such, if an offence concerns security classified information, but not national security information, the s 91.3 offence will be easier to prove than the alternative option

---

216 See *Criminal Code* s 91.11.

217 Ibid s 91.12.

218 Ibid ss 91.12 and 11.5.

219 ASIO, *ASIO Annual Report 2017–18* (n 41) 28.

of the core offence. However, the very fact that the same conduct could be caught by both offences raises questions over whether the s 91.3 offence is truly necessary. One thing is apparent, however: both the number and overlapping nature of the offences renders the 2018 espionage laws complex, unclear and confusing, suggesting that some kind of reform is needed.

In a similar vein, 61 pieces of counter-terrorism legislation were enacted in the wake of September 11 at an average rate of one new piece of legislation every 6.7 weeks.[220] Kent Roach has described this as 'hyper-legislation'.[221] Despite the existing comprehensive counter-terrorism framework, six new pieces of counter-terrorism legislation have been introduced since 2014 which criminalise an even broader range of conduct and give intelligence agencies much greater powers.[222] Australia has now enacted more counter-terrorism legislation than countries facing a greater terrorism threat, such as the United States, Canada and the United Kingdom.[223] Domestic laws also infringe more severely upon citizen's civil liberties, but this could be explained by Australia's lack of a Bill of Rights.[224] What the majority of Australian counter-terrorism legislation has in common, however, is the speed with which they were drafted, debated and enacted.[225] This is particularly problematic owing to the inherent encroachment of the laws upon individual rights and liberties.[226] Due to the hasty passing of the legislation, many new laws could not be scrutinised with sufficient care, and many problems were only realised after the laws were enacted.[227] It has since been argued that not all of these offences are necessary to combat the threat of terrorism.[228] These concerns apply equally to Australia's new espionage laws, which passed through Federal Parliament with minimal changes less than one month after the Parliamentary Joint Committee on Intelligence and Security's comprehensive 404-page Advisory Report was published.[229] The legislation also received very

---

220 Hardy and Williams (n 183) 198; McCulloch (n 185) 26.

221 Kent Roach, *The 9/11 Effect* (Cambridge University Press, 2011) 309.

222 These were developed in response to 'foreign fighters' and include declared area offences, foreign incursion offences and the ability to revoke citizenship. For a useful overview of the new terrorism offences see Hardy and Williams (n 183). See also McCulloch (n 185) 26.

223 Roach (n 221) 310; Williams, 'Legal Legacy' (n 184) 7.

224 McCulloch (n 185) 28; Kiefel (n 183) 715; Williams, 'Legal Legacy' (n 184) 11–12. Although two States now have human rights legislation: Victoria (*The Charter of Human Rights and Responsibilities Act 2006*), and Queensland (*Human Rights Act 2019*). Further analysis must be undertaken to determine whether Australia's 2018 espionage offences are compatible with these Acts.

225 Hardy and Williams (n 183) 205.

226 Ibid 207, 211.

227 Ibid 205–6.

228 Law Council of Australia, Submission to COAG, *COAG Review of Counter-Terrorism Legislation*, 27 September 2012, 10, 20; Williams, 'Legal Legacy' (n 184) 14; Hardy and Williams (n 183) 198, 205; see generally INSLM (n 184).

229 PJCIS (n 41).

little consideration by Parliament itself: the House of Representatives began its second reading debate on 26 June 2018, and by June 28th the Senate had agreed to the third reading.[230] The legislation was enacted on June 29th.[231] A very strong argument therefore exists that, similar to the suite of terrorism offences, the large number of new espionage laws were not sufficiently scrutinised before their enactment, and some may prove to be unnecessary (or disproportionate incursions on civil liberties) with time.

Australia's new espionage laws represent a unique national approach in response to the threat of espionage used in today's world. At least of the 'Five Eyes' intelligence nations,[232] Australia has been the first country to enact such harsh and sweeping espionage legislation.[233] However, it is possible that the United Kingdom will soon follow Australia's lead. In 2017, the United Kingdom Law Commission published the *Protection of Official Data: A Consultation Paper*,[234] which recommended that drastic changes be made to that nation's espionage laws. In particular, the Commission recommended that the *Official Secrets Acts 1911*, *1920* and *1939* (UK) be repealed[235] and 'replaced by more modern legislation that is designed to reflect 21st century challenges',[236] and that such legislation will be 'future proofed against developing technology and techniques in espionage'.[237]

---

230 Parliament of Australia, *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018* (30 June 2018) <https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6022>.

231 Ibid.

232 These are Australia, New Zealand, United States, Canada and United Kingdom.

233 New Zealand's sole espionage offence is found in the *Crimes Act 1961* (NZ) s 78 and prescribes a maximum penalty of 14 years' imprisonment. It has not been amended since 1983. Canada does have several espionage offences, including a preparatory offence. These are found in the *Security of Information Act* RSC 1985, c O-5, although terms are largely out-dated and penalties are mild. The United Kingdom's espionage offences are found in the *Official Secrets Acts 1911*, *1920*, *1939* and *1989* (UK) and have undergone few changes since their initial enactment. Similar to Australia, the United States has a myriad of espionage offences found in both the *Espionage Act of 1917* 37 USC and the *Economic Espionage Act of 1996* 18 USC. However, these are very specific offences that generally apply either to defence or trade secret information. They are accompanied by comparatively moderate prescribed sentences of imprisonment and have been criticised for their ambiguity and over-breadth; see Lindsay Barnes, 'The Changing Face of Espionage: Modern Times Call for Amending the Espionage Act' (2014) 46 *McGeorge Law Review* 511. For a summary of the US espionage offences, see Erin Creegan, 'National Security Crime' (2012) 3 *Harvard National Security Journal* 373. For a comparison of economic espionage laws across the Five Eyes nations, see Melanie Reid, 'A Comparative Approach to Economic Espionage: Is any Nation Effectively Dealing with this Global Threat?' (2016) 70 *University of Miami law Review* 757.

234 United Kingdom Law Commission (n 11).

235 Ibid 48.

236 UK Law Commission, *Protection of Official Data: A Consultation Paper Overview* (2017) <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2017/02/cp230_overview.pdf> 1.

237 United Kingdom Law Commission (n 11) 28.

Unlike Australia, existing espionage offences in the United Kingdom have not been modified since their introduction, including the *Official Secrets Act 1911* (UK) s 1 offence on which Australia's original espionage offence was modelled (although the United Kingdom did introduce solicitation and preparatory offences in 1920,[238] and so in this respect has long been one step ahead of Australia). The United Kingdom Law Commission suggested the following notable improvements to the United Kingdom's espionage laws: removal of archaic terms (such as reference to 'enemy');[239] use of the generic term 'information' instead of more specific terms such as 'sketch, plan, model or note';[240] replacement of 'safety or interests of the state' with 'national security';[241] criminalising communicating, obtaining and gathering information;[242] removal of restrictions on who can commit espionage;[243] and expanding the territorial ambit of the offences.[244] These recommendations have received significant and widespread criticism in the media since the Consultation Paper was published,[245] but they closely resemble the latest changes to Australia's espionage laws and may even have been the inspiration for Australia's reforms. Unlike Australia, however, the United Kingdom has not rushed into enacting new laws; the Law Commission was asked in 2015 to conduct its review, it published its Consultation Paper in 2017, and it is not due to publish its final recommendations until 2019.[246] It is hoped that some of the issues highlighted in this article regarding Australia's new espionage offences will provide useful insights to the United Kingdom Parliament when it eventually considers whether, and if so how, its nation's espionage offences should be reformed. Indeed, this analysis could prove useful to any of the Five Eyes nations.

Australia's 2018 espionage offences are scheduled to be reviewed by INSLM in 2021.[247] At that time, it is recommended that INSLM carefully consider whether all of the offences are truly necessary, and/or whether they could be simplified in some way. For example, conduct targeted by some of the offences that is

---

238 *Official Secrets Act 1920* (UK) s 7.

239 United Kingdom Law Commission (n 11) 30–2.

240 Ibid 33.

241 Ibid 34–5.

242 Ibid 33.

243 Ibid.

244 Ibid 44–5.

245 See above n 12.

246 UK Law Commission, *Protection of Official Data Current Project Status* (2018) <http://www.lawcom.gov.uk/project/protection-of-official-data/#protection-of-official-data>.

247 *Independent National Security Legislation Monitor Act 2010* (Cth) s 6(1B) ('*INSLM Act*'). The INSLM independently reviews the operation, effectiveness and implications of national security and counter-terrorism laws, and considers whether the laws contain appropriate protections for individual rights, remain proportionate to terrorism or national security threats, and remain necessary: *INSLM Act 2010* (Cth) s 6(1).

considered more severe could be added to the list of aggravating circumstances, instead of existing as standalone offences. This could include espionage conducted specifically on behalf of a foreign principal.[248] Similarly, mitigating factors could be included to decrease penalties for less severe conduct than the core offence, again instead of existing as separate offences. This could include, for example, the mental element of recklessness (instead of intention)[249] or conduct targeted by the s 91.2 offences where information need not actually concern Australia's national security and may not be true but the person still possessed the requisite fault element to prejudice Australia's national security.[250] Given the breadth of conduct caught by these offences (some of which may have an innocent explanation), it may also be apt to require the Attorney-General to consent to prosecutions under the offences. It is recommended that at the time of review of the offences, INSLM also conduct a thorough assessment into the breadth of the offences and their impact on human rights and the rule of law.

VI Conclusion

Only time will tell which, if any, of the 27 new espionage offences in the *Criminal Code* will effectively address espionage used in today's world. Detailed examination of the core, solicitation and preparatory offences indicates that the core offence is necessary to effectively address espionage used today in terms of being sufficiently broad to capture today's espionage practices. Moreover, the solicitation and preparatory offences are likely to be effective, as they will be sufficiently easy to prove and carry relatively severe penalties to support convictions and deter others from engaging in espionage. However, the number and breadth of the offences do raise concerns regarding their impact on human rights and the rule of law. These issues, as well as other costs associated with the new offences, should be investigated thoroughly. In light of the current known threat of espionage against Australia, it is hoped that law enforcement will take the initiative to use the legislative tools they now have to effectively address and adapt to the serious threats posed by the espionage of today.

248 *Criminal Code* s 91.8.
249 See ibid ss 91.1(2), 91.2(2), 91.8(2).
250 Ibid s 91.2.