Report on the impact on journalists of section 35P of the ASIO Act

October 2015

The Hon Roger Gyles AO QC
© Commonwealth of Australia 2015


ISBN 978-1-925238-00-6 Report on the impact on journalists of section 35P of the ASIO Act (PDF)


Copyright notice

With the exception of the Commonwealth Coat of Arms, this work is licensed under a Creative Commons Attribution 3.0 Australia licence (CC BY 3.0) (http://creativecommons.org/licenses/by/3.0/au/deed.en).

This work must be attributed as: ‘Commonwealth of Australia, Department of the Prime Minister and Cabinet, Report on the impact on journalists of section 35P of the ASIO Act.’

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the following website: http://www.itsanhonour.gov.au/coat-arms/.

Enquiries regarding the licence and any use of this work are welcome at:

The Independent National Security Legislation Monitor
via the Department of the Prime Minister and Cabinet
PO Box 6500 Canberra ACT 2600
+61 2 6271 5111
www.dpmc.gov.au
Report on the impact on journalists of section 35P of the ASIO Act
## Contents

Preface ......................................................................................................................... 1  
Executive summary ..................................................................................................... 2  
Context ........................................................................................................................ 5  
Reasoning and conclusions.......................................................................................... 8  
Appendix A—List of contributors to the inquiry .......................................................29  
Appendix B—Legislative history of section 35P ........................................................33  
Appendix C—Post-enactment safeguards....................................................................56  
Appendix D—A selection of criticisms and comments about section 35P from submissions to the inquiry .................................................................63  
Appendix E—A selection of proposals for reform from submissions to the inquiry .................................................................................................................................66  
Appendix F—AGD and ASIO response to certain criticisms ....................................73  
Appendix G—A selection of comments about oversight and the role of the IGIS in submissions to the inquiry ............................................................83  
Appendix H—Brief history of ASIO and the ASIO Act ............................................87  
Appendix I—ASIO public accountability .................................................................96  
Appendix J—Relevant constitutional and international law ...................................102  
Appendix K—The controlled operations precedent for the SIO scheme and section 35P ......................................................................................................................117  
Appendix L—History of Commonwealth secrecy offences ..................................131  
Appendix M—Existing Commonwealth secrecy offences: official comments ......150  
Appendix N—SIOs and protecting information: international comparisons ........158  
Abbreviations ..........................................................................................................173
Preface

The report is the result of a Reference from the Prime Minister under section 7 of the Independent National Security Legislation Monitor Act 2010 (INSLM Act) and is provided pursuant to section 30(1) of the INSLM Act.

I invited submissions through a public advertisement and direct invitation to a broad range of interested parties. Submissions closed on 20 April 2015, with a total of 41 submissions received.¹ I also requested and received a range of information and documents from relevant agencies. In addition, hearings were held pursuant to section 21 of the INSLM Act. Some parts of the hearings were held in private, where sensitive operational issues were discussed.

The submissions, information received and transcripts of the public hearings are available at http://www.dpmc.gov.au/pmc/about-pmc/core-priorities/independent-national-security-legislation-monitor. As a result, it is not necessary to reproduce that material in full in this report and only key aspects are summarised in the Appendixes.² The report focuses on the material that is critical to the conclusions reached.

I would like to acknowledge the assistance of successive advisers, particularly Mr Charles Beltz, and the administrative assistance provided by the Department of the Prime Minister and Cabinet in conducting the inquiry and preparing this report.

The Hon Roger Gyles AO QC
Independent National Security Legislation Monitor

¹ Appendix A lists persons and groups who made submissions to the inquiry and who met with the Independent National Security Monitor (INSLM) in connection with this inquiry.
² Appendix B describes the legislative history of section 35P and sets out relevant parts of the Explanatory Memorandum to the National Security Legislation Amendment Bill (No 1) 2014 (NSLAB (No 1) 2014). This Appendix is the main avenue by which this report reflects the official explanation and justification for section 35P (but see also Appendix F, which summarises responses by the Attorney-General’s Department and ASIO to certain criticisms, and Appendix M, which contains some official comments about existing secrecy offences). Appendix D sets out some criticisms and comments about section 35P from submissions received while Appendix E sets out some proposed ways to remedy criticisms of section 35P from submissions received.
Executive summary

Purpose

This report discusses the impact on journalists of the operation of section 35P of the Australian Security Intelligence Organisation Act 1979 (ASIO Act) concerning offences for the disclosure of information relating to a special intelligence operation (SIO).

Impact

The impact of section 35P on journalists is twofold:

A. It creates uncertainty as to what may be published about the activities of ASIO without fear of prosecution. The so-called chilling effect of that uncertainty is exacerbated because it also applies in relation to disclosures made to editors for the purpose of discussion before publication.

B. Journalists are prohibited from publishing anywhere at any time any information relating to an SIO, regardless of whether it has any, or any continuing, operational significance and even if it discloses reprehensible conduct by ASIO insiders.4

Issues

The basic problem with section 35P is that it does not distinguish between journalists and others (outsiders) and ASIO insiders. The application in this manner of broad secrecy prohibitions to outsiders is not satisfactorily justified, including by precedents in Australia or elsewhere.

The SIO scheme is necessary and proportionate to the present threats to security. The statutory and administrative procedures in force are appropriate safeguards against abuse. A secrecy provision relating to the scheme is not inappropriate. However, section 35P is not justified. It does not contain adequate safeguards for protecting the rights of outsiders and is not proportionate to the threat of terrorism or the threat to national security.

3 This report assumes that the Commonwealth authorities are correct in contending that ‘disclose’ in section 35P covers all communication of information of the requisite kind by anybody to anybody else regardless of the knowledge of either party as to that information.

4 ‘Insiders’ include ASIO employees, contractors and people who have entered into an agreement or arrangement with ASIO. ‘Outsiders’ are third parties such as journalists.
Section 35P is arguably invalid on the basis that it infringes the constitutional protection of freedom of political communication. Section 35P is also arguably inconsistent with article 19 of the *International Covenant on Civil and Political Rights* and so not in accordance with Australia’s international obligations.

Three basic flaws need to be addressed. The first is the absence of an express harm requirement for breach (of the basic offence) by a journalist or other third party. The second is that recklessness is the fault element in relation to the circumstance described in section 35P(2)(c)(ii) (that is, in relation to the latter harm requirement in the aggravated offence). The third is the prohibition of disclosure of information already in the public domain.

**Recommendations**

Section 35P should be redrafted to treat insiders and outsiders separately, with one part dealing with third parties and another part dealing with insiders. There should be a basic offence (penalty five years imprisonment) and an aggravated offence (penalty 10 years imprisonment) in relation to both insiders and outsiders.

**Insiders**
The basic offence and the aggravated offences for insiders would be as per current section 35P.

**Outsiders**
The basic offence for outsiders would have the same elements as section 35P(1), but with the additional physical element that the disclosure of the information will endanger the health or safety of any person or prejudice the effective conduct of an SIO. Recklessness would be the default fault element in relation to this last physical element.

The aggravated offence for outsiders would have the same elements as section 35P(2) except that the fault element for (c)(ii) should be knowledge rather than recklessness (in other words, the fault element for the circumstance that the disclosure will endanger the health or safety of any person or prejudice the effective conduct of the operation should be specified to be knowledge).

There should be a defence of prior publication (not available to a member or ex-member of the intelligence and security services in respect of information available to them in that capacity).
This defence should require the defendant to satisfy the court that:

- the information in question had previously been published
- having regard to the nature and extent of that prior publication and the place where it occurred, the defendant had reasonable grounds to believe that the second publication was not damaging, and
- the defendant was not in any way directly or indirectly involved in the prior publication.
Context

The Reference

On 11 December 2014, in conjunction with my appointment as the Acting Independent National Security Legislation Monitor (INSLM)\(^5\), the Prime Minister referred the following matter to me pursuant to section 7 of the Independent National Security Legislation Monitor Act 2010 (INSLM Act):

\[\ldots\text{any impact on journalists in the operation of section 35P of the Australian Security Intelligence Organisation Act 1979 concerning offences for the disclosure of information relating to a ‘special intelligence operation’, as inserted by the National Security Legislation Amendment Act (No 1) 2014.}\]

This report on the Reference is provided pursuant to section 6(1)(c) and section 30(1) of the INSLM Act.

Considerations

In conducting the Reference I needed to keep in mind the object of the INSLM Act set out in section 3, particularly in this context section 3(c) and (d):

\[\text{The object of this Act is to appoint an Independent National Security Legislation Monitor who will assist Ministers in ensuring that Australia's counter-terrorism and national security legislation:}\]

\[\text{(c) is consistent with Australia's international obligations, including:}\]

\[(i)\text{ human rights obligations; and}\]
\[(ii)\text{ counter-terrorism obligations; and}\]
\[(iii)\text{ international security obligations; and}\]

\[\text{(d) contains appropriate safeguards for protecting the rights of individuals.}\]

I also needed to bear in mind section 6(1)(b) of the INSLM Act, which describes a function of the INSLM as follows:

\[\text{(b) to consider, on his or her own initiative, whether any legislation mentioned in paragraph (a):}\]

\[(i)\text{ contains appropriate safeguards for protecting the rights of individuals; and}\]

\[\]

\(^5\) Mr Gyles was appointed as INSLM (non-acting) for a two-year term on and from 20 August 2015.
(ii) remains proportionate to any threat of terrorism or threat to national security, or both; and
(iii) remains necessary.

In addition, I needed to consider section 8 of the INSLM Act, which provides:

When performing the Independent National Security Legislation Monitor’s functions, the Monitor must have regard to:

(a) Australia’s obligations under international agreements (as in force from time to time), including:
   (i) human rights obligations; and
   (ii) counter-terrorism obligations; and
   (iii) international security obligations; and

(b) arrangements agreed from time to time between the Commonwealth, the States and the Territories to ensure a national approach to countering terrorism.

The meaning of ‘journalists’

A threshold question for the purposes of this Reference is what is meant by the word ‘journalists’.

The Macquarie Dictionary defines ‘journalist’ as ‘one engaged in journalism’ and relevantly defines ‘journalism’ as ‘the occupation of writing for, editing and producing newspapers and other periodicals, and television and radio shows’. Other definitions of ‘journalist’ include ‘one who keeps a journal’ (Free Dictionary) and of ‘journalism’ include ‘the activity of gathering, creating, and presenting news and information’ (American Press Institute).

Some Commonwealth laws which refer to ‘journalist’ clearly apply only to ‘professional’ journalists:

- The crime created by section 119.2 of the Criminal Code (entering, or remaining in, declared areas) has an exception for a person who enters, or remains in, the area solely for the purpose of making a news report of events in the area, where the person is working in a professional capacity as a journalist.
- The same basic approach is taken in relation to ‘journalist information warrants’, which may be issued under changes to the Telecommunications (Interception and Access) 1979 made by the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 and
effective from 13 October 2015 (see section 180G and section 5(1) definition of ‘source’).

For the purposes of the ‘shield’ law in section 202 of the Broadcasting Services Act 1992, the term ‘journalist’ is defined in section 202(5) to mean a person engaged in the profession or practice of reporting for, photographing, editing, recording or making television or radio programs, or datacasting content, of a news, current affairs, information or documentary character.

By comparison, the following definitions apply for the purposes of the ‘shield’ law in section 126H of the Evidence Act 1995, which is designed to give presumptive protection to journalists against having to disclose, in legal proceedings, the identity of confidential informants:

- ‘journalist’ means a person who is engaged and active in the publication of news and who may be given information by an informant in the expectation that the information may be published in a news medium
- ‘informant’ means a person who gives information to a journalist in the normal course of the journalist’s work in the expectation that the information may be published in a news medium, and
- ‘news medium’ means any medium for the dissemination to the public or a section of the public of news and observations on news.

That language seems potentially to encompass a broader range of ‘journalists’ than the other Commonwealth laws mentioned. For example, an article entitled Democracy in Australia—Protection of journalists and their sources published by the Australian Collaboration, states:

The federal shield law applies to anyone who is ‘engaged and active in the publication of news’, including bloggers, tweeters, aggregators and email campaigners. The law also protects those publishing in a ‘news medium’, defined as ‘any’ medium of dissemination to the public.

The same article contrasts federal shield law with New South Wales shield law, which restricts the definition of a ‘journalist’ to a person ‘engaged in the profession or occupation of journalism’.
However, the Explanatory Memorandum to the Evidence Amendment (Journalists’ Privilege) Bill 2010, which became the relevant amending Act in 2011, states that the protection operates alongside the *Australian Journalists Association Code of Ethics*, and that:

> It is also significant to note that the journalist should be operating in the course of their work. This means that the journalist should be employed as such for the privilege to operate, and private individuals who make postings on the internet or produce non-professional news publications, where this is not their job, will not be covered by section 126H.

There may be some difficulties applying this test of a ‘journalist’ in some cases, for example, in relation to freelance or self-employed commentators including internet bloggers, who may be remunerated for intermittent reporting work.

Given the circumstances leading to this Reference (see paragraphs 30-31 below and Appendix B), this inquiry proceeded on the basis that ‘journalists’ in this Reference refers to professional journalists, recognising that there will be debate as to the boundaries of that description. Further, the inquiry focused on journalists operating independently of the Government.

**Reasoning and conclusions**

**What does section 35P prohibit?**

1. The basic offence created by section 35P of the ASIO Act is as follows:  

   **Unauthorised disclosure of information**
   
   (1) A person commits an offence if:
   
   (a) the person discloses information; and
   
   (b) the information relates to a special intelligence operation.

   **Penalty:** Imprisonment for 5 years.

   **Note:** Recklessness is the fault element for the circumstance described in paragraph (1)(b)—see section 5.6 of the *Criminal Code*.

2. Section 35P(2) comprises an aggravated version of the basic offence, with an express harm requirement.

---

6 Section 35P is set out in full at the end of Appendix B, which describes the legislative history of the section.
3. There is no special definition of ‘information’—it bears its ordinary meaning. According to the *Macquarie Dictionary*, ‘information’ relevantly means ‘1. Knowledge communicated or received concerning some fact or circumstance; news. 2. Knowledge on various subjects, however acquired’.

4. Section 4 of the ASIO Act provides that, unless the contrary intention appears:

   *special intelligence conduct* means conduct for or in relation to which a person would, but for section 35K, be subject to civil or criminal liability under a law of the Commonwealth, a State or a Territory.

   *special intelligence function* means a function of the Organisation under paragraph 17(1)(a), (b), (e) or (f)

   *special intelligence operation* is an operation:

   (a) in relation to which a special intelligence operation authority has been granted; and
   (b) that is carried out for a purpose relevant to the performance of one or more special intelligence functions; and
   (c) that may involve an ASIO employee or an ASIO affiliate in special intelligence conduct.

   *special intelligence operation authority* means an authority to conduct a special intelligence operation granted under section 35C.

5. Section 17 of the ASIO Act, so far as is relevant, provides:

   **17 Functions of Organisation**

   (1) The functions of the Organisation are:
   (a) to obtain, correlate and evaluate intelligence relevant to security;
   (b) for purposes relevant to security, to communicate any such intelligence to such persons, and in such manner, as are appropriate to those purposes;
   ...
   (e) to obtain within Australia foreign intelligence pursuant to section 27A or 27B of this Act or section 11A, 11B or 11C of the *Telecommunications (Interception and Access) Act 1979*, and to communicate any such intelligence in accordance with this Act or the *Telecommunications (Interception and Access) Act 1979*; and
   (f) to co-operate with and assist bodies referred to in section 19A in accordance with that section.
6. There is no special definition of ‘intelligence’—it bears its ordinary meaning. According to the *Macquarie Dictionary*, ‘intelligence’ relevantly means ‘5. Knowledge of an event, circumstance etc., received or imparted; news; information. 6. The gathering or distribution of information, especially secret information which might prove detrimental to an enemy’.

7. The meaning of the word ‘intelligence’ as used in the ASIO Act may also be informed by the discussion of such matters in the Royal Commission on Intelligence and Security (RCIS), conducted by Justice Hope between 1974 and 1977. The RCIS was the catalyst for the ASIO Act (some significant aspects of the RCIS are discussed in Appendix H of this report). There is also a useful consideration of ASIO ‘intelligence’ and ‘information’ in *R v Thomas* (No 4) 2008 VSCA 107 (paragraphs 13–22). For present purposes, it is sufficient to say that each of these words has a very broad meaning.

8. An SIO is an operation carried out for a purpose relevant to the performance of a ‘special intelligence function’. These are the functions in section 17 set out in paragraph 5 above.

9. A person may commit an offence under section 35P if the person ‘discloses’ information which ‘relates to’ an SIO. The ordinary meaning of ‘disclose’ is to reveal something that is known by the discloser and not previously known to the person to whom the disclosure is made (see *Nasr v New South Wales* (2007) 70 A Crim R 78 at 106 and the various other cases cited there; see further *Ashby v Commonwealth* (2012) 203 FCR 440 at [30] and 31], a case which concerned the availability of journalists’ privilege in circumstances where the identity of a confidential source may already have been revealed). The Explanatory Memorandum to the National Security Legislation Amendment Bill (No 1) 2014 (NSLAB (No 1) 2014) says that ‘disclose’ is intended to take its ordinary meaning. However, it indicates that to ‘disclose’ is intended to include the making available of information to others by any means. It says that it is not intended to require, as a rule, proof that the information was received by another person, or that another person read, heard or viewed the information. The Attorney-General’s Department (AGD) and ASIO also submitted to this inquiry that section 35P is intended to apply even to a disclosure of information already in the public domain.

---

7 See for example paragraphs 125–256 and 666–680 of the Fourth Report, Vol 1 of the RCIS.
10. The wide view now taken of the word ‘disclose’ in section 35P is certainly contestable. It would encompass passing on information that the discloser would not know to be true. It would also encompass passing information to a recipient who was already aware of the same information. This is stretching the ordinary meaning. ‘Disclose’ is apt to deal with a communication from an insider with knowledge of an SIO to those with no such knowledge. Wider dissemination would more naturally be captured by words such as ‘communicate’ or ‘publish’. Other ASIO Act provisions refer to the communication (section 18(2)) or publication (section 92) of information, rather than the disclosure of information. The fact that section 35P does not distinguish between ASIO insiders and third parties (including journalists) points in the direction of a narrower meaning. The proper construction of section 35P must await a judicial determination. The result cannot be safely predicted. In the meantime, journalists would assume that the wide official position will guide decisions as to prosecution.

11. The connecting phrase in section 35P, ‘relates to’, is broad. According to *HP Mercantile Pty Ltd v Commissioner of Taxation* (2005) 143 FCR 555:

   It was common ground that the words ‘relates to’ are wide words signifying some connection between two subject matters. The connection or association signified by the words may be direct or indirect, substantial or real. It must be relevant and usually a remote connection would not suffice. The sufficiency of the connection or association will be a matter for judgment which will depend, among other things, upon the subject matter of the enquiry, the legislative history, and the facts of the case. Put simply, the degree of relationship implied by the necessity to find a relationship will depend upon the context within which the words are found.

12. An SIO is a kind of ‘operation’. That term is not defined and would bear its ordinary meaning, in this statutory context. According to the *Macquarie Dictionary*, ‘operation’ relevantly means ‘1. The act, process or manner of operating... 4. Exertion of force or influence; agency. 5. A process of a practical or mechanical nature in some form of work or production: a delicate operation in watchmaking.... 7. A particular course or process: mental operations... 11. Military, Navy a. the conduct of a campaign. b. a campaign’. In essence, an operation involves activities directed to a particular end.

13. That which marks out an SIO from other ASIO operations is the authority granted to break the law. The covert nature of an SIO is not a distinguishing feature of it. All ASIO activities carried out for a purpose relevant to a ‘special
intelligence function’ as defined involve covert intelligence gathering. The covert involvement of human sources is not a distinguishing feature of an SIO. The method of intelligence gathering and the nature of the authorised illegal activity are not limited by the legislation. The effect of the legislation must be judged by the width of potential operation rather than any subset of it.

14. An SIO need not be an anti-terrorism operation. As indicated above, it may support other functions of ASIO, including counter-espionage.

**What is the impact on journalists?**

15. This analysis demonstrates the width of the connection between ‘information’ and an SIO. Accordingly, a large and imprecise range of material would be caught, some (perhaps much) of it with no, or no continuing, operational significance. The prohibition is not limited by time or space and extends to information known to be public. This would make it difficult for journalists to report. The difficulty is compounded because in practice journalists should not know of the existence of an SIO (let alone the details). It is contended on behalf of ASIO that disclosure may be authorised by the Director-General, who has control of ASIO (section 8(1)), in accordance with the performance of the functions and duties, or the exercise of the powers, of ASIO (section 35P(3)(d)). Even if this is correct and could include disclosure to a journalist, the invariable practice of ASIO has been to decline to comment on operational matters.

16. The impact of section 35P on journalists is twofold.

17. **The first impact is uncertainty as to what journalists may publish about the activities of ASIO without fear of prosecution.** As described in the notes to section 35P, recklessness is the fault element for the circumstance described in paragraph (1)(b) and (2)(b)—namely, that the information relates to an SIO. In other words, the prosecution must prove that the person was reckless as to the circumstance that the information relates to an SIO. In this context, section 5.4 of the *Criminal Code* provides:

   (1) A person is reckless with respect to a circumstance if:
       (a) He or she is aware of a substantial risk that the circumstance exists or will exist; and
       (b) Having regard to the circumstances known to him or her, it is unjustifiable to take the risk.

   ...
The question whether taking a risk is unjustifiable is one of fact.

If recklessness is a fault element for a physical element of an offence, proof of intention, knowledge or recklessness will satisfy that fault element.

18. This presents a significant challenge in any prosecution.8 Inadvertence would not qualify. However, recklessness can be established in the absence of knowledge. It may be difficult for a person, including a journalist, to decide whether they risk prosecution by making a particular disclosure.9

19. What would be the effect of ASIO refusing to comment on a journalist’s enquiry? It is arguable that a subsequent disclosure would not be reckless. On the other hand, it could be argued that if the journalist knew of the invariable practice of ASIO not to comment, the enquiry would be of no substance. The media is also concerned that if the enquiry was answered by affirming a link with an SIO, there would be no means of verifying the assertion,10 yet publishing in the face of it would probably be considered reckless.

20. The result is that reporting on ASIO activities is something of a lottery, although the risk may have been exaggerated in some submissions.11 The uncertainty at the point of possible publication could well have a chilling effect on dissemination of material about security and ASIO’s conduct with no relevant connection to an SIO. This effect may also extend to inhibiting pre-publication

---

8 See, for example, pages 5–10 of Submission 19 to this inquiry (from the Commonwealth Director of Public Prosecutions), pages 26–27 of Submission 8 to this inquiry (a joint submission from the AGD and ASIO) and page 14 of Submission 24 to this inquiry (from the AGD, responding to requests for information).

9 As legal advice forming part of Submission 1 to this inquiry (from Seven West Media) notes, where a journalist does not actually know that information relates to an SIO, the question is whether the journalist is aware of a substantial risk that it does relate to an SIO and, if so, whether it is unjustifiable to take the risk. The latter is a factual question whose answer depends on all the circumstances. This and other submissions state that publishing information concerning counter-terrorism and other intelligence operations involving ASIO (or, in some cases, other agencies), in the absence of confirmation that the information relates to an SIO, risks breaching section 35P.

10 See, for example, paragraph 68 of Attachment 2 and supplementary submission No 2 to Submission 1 to this inquiry (from Seven West Media).

11 In practice, prosecuting secrecy offences, particularly in a national security context, has been quite rare and difficult (although that may not always remain the case). Submissions to this inquiry, including from relevant Commonwealth authorities, suggest that no journalist has been prosecuted for a Commonwealth secrecy offence. See also Appendix L, which mentions some prosecutions of intelligence insiders.
discussions about the same material, for example between journalists and their editors.

21. Whether disclosure by a journalist (or other person) to a lawyer for advice about further disclosures by publication or otherwise is prohibited depends on the proper construction of section 35P(3)(e), which provides that the offences do not apply to a disclosure ‘for the purpose of obtaining legal advice in relation to the special intelligence operation’. The explanatory material indicates that a purpose of the exception was to allow non-participants\(^{12}\) to seek legal advice about suspected activities of ASIO in relation to them.\(^{13}\) Section 35P(3)(e) does not expressly refer to legal advice in relation to the matter of the subject of the offence, that is, the disclosure.\(^{14}\) The width of the phrase ‘in relation to’ suggests that the provision would protect disclosure by a journalist for the purpose of obtaining legal advice about a proposed publication, but that will remain moot until determined by a court.

22. The second, and more fundamental impact, is that journalists are prohibited from publishing anywhere,\(^{15}\) at any time, any information relating to an SIO, regardless of whether it has any, or any continuing, operational significance and even if there was reprehensible conduct by ASIO employees or affiliates. In this regard, the journalist’s source is not pertinent (it does not matter whether the information came from an insider/whistleblower, an outsider/computer hacker or from some other source).

23. This is a major departure from the position which has generally prevailed to date in relation to ASIO’s activities. That position is that ASIO employees, contractors and persons who have entered into an agreement or arrangement with ASIO (described as ‘insiders’) are subject to stricter secrecy provisions than outsiders. Section 18(2) of the ASIO Act has always applied in relation to all

\(^{12}\) For the purpose of the SIO scheme, the ASIO Act (section 4) defines a ‘participant’ in an SIO, subject to a contrary intention, as a person authorised to engage in special intelligence conduct for the purposes of an SIO. All other persons may be referred to as ‘non-participants’.

\(^{13}\) See paragraph 578 of the Explanatory Memorandum to the NSLAB (No 1) 2014 and paragraph 3.102 of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) Report in relation to that Bill, extracts of which are in Appendix B, and page 42 of the joint AGD/ASIO submission of August 2014 to the PJCIS inquiry.

\(^{14}\) See Submission 14 to this inquiry (from Australian Lawyers for Human Rights).

\(^{15}\) The effect of section 35P(4) is that the offences apply to any person in respect of conduct which takes place in any country, see paragraph 586 of the Explanatory Memorandum to the NSLAB (No 1) 2014.
such persons and, broadly, prohibits the unauthorised disclosure of ASIO information. The only sections of the ASIO Act having a direct impact on ‘outsiders’ such as journalists are section 92 and the relatively new section 34ZS. Section 79 of the Crimes Act prohibits the unauthorised receipt of confidential information. However, section 79(3) (which deals with disclosures) has been ineffective in relation to secondary disclosures, including publication, by third parties because of the need to identify a duty on the part of the person concerned to keep the relevant information secret. It appears that few if any journalists have ever been prosecuted for a secrecy offence, either in the context of the controlled operations scheme or for any other Commonwealth secrecy offence relevant in the present context.

24. The aggravated offence in section 35P(2) creates an additional problem for journalists (or other outsiders). It reads:

*Unauthorised disclosure of information—endangering safety, etc.*

(2) A person commits an offence if:

(a) the person discloses information; and
(b) the information relates to a special intelligence operation; and
(c) either:

(i) the person intends to endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation; or
(ii) the disclosure of the information will endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation.

Penalty: Imprisonment for 10 years.

Note: Recklessness is the fault element for the circumstance described in paragraph (2)(b) —see section 5.6 of the *Criminal Code*.

Recklessness is also the fault element applicable to paragraph (c)(ii). Thus a journalist with no knowledge or means of knowledge about the SIO, or the effect disclosure would have, would risk imprisonment for 10 years if held to be reckless as to both elements.

---

16 Section 92 was an original provision of the ASIO Act (see Appendix H). It broadly prohibits a person from making public the identity of a current or former ASIO employee or ASIO affiliate.

17 The need for reform of the Crimes Act secrecy offences is widely recognised (see Appendix L).
25. These impacts on journalists are not eliminated by any defences or exceptions in the event of publication.\textsuperscript{18} There is no time limit on the prohibition. The ability to report matters to the Inspector-General of Intelligence Services (IGIS), while an important safeguard against wrongdoing by ASIO, is not a substitute for the role of the media\textsuperscript{19} and exercising freedom of speech.

26. The impact on journalists of the operation of section 35P is ameliorated to some extent. The Commonwealth Director of Public Prosecutions (CDPP) takes into account the public interest in making a disclosure when deciding whether to prosecute a person. The following directions\textsuperscript{20} have been made in this context:

- on 29 October 2014 the CDPP issued a National Legal Direction, \textit{Prosecuting offences for unauthorised disclosure of information relating to controlled operations, special intelligence operations or delayed notification search warrants}, requiring prosecutors to seek the personal approval of the CDPP to any proposed prosecutions of offences against section 35P, and
- on 30 October 2014 the Attorney-General issued a direction to the CDPP under section 8 of the \textit{Director of Public Prosecutions Act 1983} requiring the CDPP to obtain the consent of the Attorney-General to prosecute a journalist for certain offences including offences against section 35P, where the facts constituting the alleged offence relate to the work of the person in a professional capacity as a journalist.

27. While these measures should give some comfort to journalists, they are after the event of publication and depend on the exercise of a discretion. They do not provide a defence, or a legal guarantee of immunity from prosecution. The

\textsuperscript{18} The exceptions in section 35P(3) apply if the disclosure was:
(a) in connection with the administration or execution of this Division; or
(b) for the purposes of any legal proceedings arising out of or otherwise related to this Division or of any report of any such proceedings; or
(c) in accordance with any requirement imposed by law; or
(d) in connection with the performance of functions or duties, or the exercise of powers, of the Organisation; or
(e) for the purpose of obtaining legal advice in relation to the special intelligence operation; or
(f) to an IGIS official for the purpose of the Inspector-General of Intelligence and Security exercising powers, or performing functions or duties, under the \textit{Inspector-General of Intelligence and Security Act 1986}; or
(g) by an IGIS official in connection with the IGIS official exercising powers, or performing functions or duties, under that Act.

\textsuperscript{19} See Appendix G, which contains a selection of comments on oversight and an extract from the submission of the IGIS in relation to this inquiry.
\textsuperscript{20} The precise terms of these directions are set out in Appendix C.
rest of the community, including those affected by ASIO operations and commentators of all kinds, such as academics and bloggers, are subject to the same impact as journalists. The question of whether a person is a ‘journalist’ only becomes critical when there are special rules or procedures applicable in relation to ‘journalists’.

28. This inquiry considered whether it might be helpful to have a form of pre-publication clearance or a variation of the former D-notice regime (the defunct D-Notice System and the extant DSMA-Notice System in the United Kingdom are discussed in Appendix N of this report). There was no real enthusiasm displayed by the media or ASIO for any such solution. No detailed proposal was put forward that could deal with the difficulties of devising such a scheme.

**This impact must be justified**

29. The understanding in the community as to the role of the media in disclosing matters of public interest, together with aspects of constitutional law and international law, require that any restriction on freedom of expression by journalists should be proportional to maintaining national security.

**Where does section 35P come from?**

30. The provenance of section 35P lies in sections 15HK and 15HL of the Crimes Act, which were inserted into Part IAB of the Act dealing with controlled operations in 2010. Part IAB permitted authorisation of illegal conduct in the investigation of drug trafficking cases. It was introduced in 1996 as a response to the High Court decision in *R v Ridgeway*, where illegally-obtained evidence was excluded. It was extended to other offences in 2001, including offences involving espionage and threats to national security. There was no stand-alone secrecy provision in Part IAB. The 2010 amendments established a national (controlled operations) scheme. A review of the material concerning

---

21 Appendix J discusses constitutional matters relevant to criminalising communication, particularly in relation to governmental matters. There is an implied freedom of political communication in the Australian Constitution, which acts as a restraint on the legislative power of the Parliament.

22 Appendix J discusses international law matters relevant to criminalising communication, particularly in relation to governmental matters. Australia is a signatory to the International Covenant on Civil and Political Rights, Article 19 of which provides for freedom of expression including the right ‘to seek, receive and impart information and ideas of all kinds regardless of frontiers’, subject to certain exceptions.

23 See Appendix K, which discusses the genesis of the controlled operations scheme and the secrecy provisions it contains.
the development of that scheme does not reveal any rigorous examination of the secrecy provisions, particularly how they might relate to existing secrecy provisions or what impact they would have on freedom of expression. Neither was there any examination of how those provisions could be reconciled with prior reports of the Review of Commonwealth Criminal Law (the Gibbs Committee), the Commission of Inquiry into the Australian Secret Intelligence Service (ASIS) and the Australian Law Reform Commission (ALRC). In this regard, in Report No 112, Secrecy Laws and Open Government in Australia, the ALRC generally:

- accepted that harm was implicit in any disclosure of information obtained or generated by intelligence agencies
- accepted that specific secrecy offences could be justified in this context (the ALRC recommended that many secrecy offences be abolished and a new general secrecy offence be created)
- recognised in this context a distinction between secrecy offences directed specifically at insiders (who have special duties to maintain secrecy) and those capable of applying to all persons, and
- recommended that secrecy offences capable of applying to persons other than insiders have an express harm requirement.

31. The SIO scheme arose out of a recommendation in a 2013 Parliamentary Joint Committee on Intelligence and Security (PJCIS) Report that the ASIO Act should be amended to create an authorised intelligence operations scheme, adapted from the Crimes Act controlled operations scheme. Neither that report nor the preceding discussion paper referred to secrecy provisions. The second reading speech and the Explanatory Memorandum for the bill that introduced Division 4 of Part III in 2014 refer briefly to section 35P without noting or justifying extension of criminal sanctions for breach of secrecy to third parties or the lack of distinction between third parties and ASIO insiders. Section 35P generated significant controversy and criticism, particularly from the media. There was greater scrutiny of section 35P in later deliberations of the Senate Standing Committee for the Scrutiny of Bills and the Parliamentary Joint Committee on Human Rights, as noted in Appendix B.

---

24 See Appendix L, which summarises the main relevant findings and recommendations of these reports.
Conclusions in relation to precedents for section 35P

32. The Crimes Act precedent is not sufficient to justify section 35P. Apart from the fact that there was no real examination of the merits of the extension of secrecy in relation to that scheme, police operations deal with a much greater range of crimes than only those crimes which relate to national security (such as terrorist offences). Further, police operations are aimed at gathering evidence to support law enforcement through prosecution, rather than intelligence gathering per se. Of greater weight in favour of section 35P is the fact that there have been numerous controlled operations conducted since 2010 without media or other criticism. No submission to this inquiry by or on behalf of a journalist or media organisation said that material was not published because of the controlled operations secrecy sections in the Crimes Act, and no prosecutions have been brought or considered. However, it has only been five years since 2010, and the media and other parties now interested do not seem to have been conscious of the secrecy provisions, and may not have become aware of any controlled operation. Also, informal contacts between police and journalists are routine and may have averted any problem.

33. Neither section 92 nor section 34ZS (referred to in paragraph 23 above) provide a satisfactory precedent for section 35P. Each is a more closely targeted provision, drafted differently from section 35P. Potential harm to individuals is built in to section 92, which applies generally. Section 34ZS does not prohibit disclosure of a broad range of information for all time and furthermore, section 34ZS was not subjected to the close examination that section 35P has received. If that had occurred, problems of the kind identified in relation to section 35P would have emerged.

Overseas experience

34. Is section 35P justified by overseas precedents or experience? Analysing the situation in other jurisdictions is difficult. The security landscape varies from place to place, which makes comparisons difficult. No clear or convincing external precedent has been identified.

---

25 See Submission 19 to this inquiry (from the CDPP), pages 1–2.
26 See Appendix N.
Intelligence operations experience

35. There has been insufficient experience of SIOs from which to draw any relevant conclusions. However, as pointed out, an SIO only varies from other ASIO activities in that illegal behaviour is authorised. ASIO’s position is that an SIO will be reserved for the most serious investigations. The formalities and procedures to be followed before, during and after an SIO and the limitations on conduct that can be authorised support that position. It is also noted that no case has been made that media or other third-party disclosures have compromised other covert ASIO operations over the years.

Place of section 35P in context

36. There is much in the objections in principle to making it a criminal offence for journalists (and others) to publish information relating to activities by or on behalf of ASIO. At first sight, it seems anomalous to do so where illegality is authorised. However, the focus on section 35P skews the argument. The real questions are whether the SIO scheme reflected in Division 4 of Part III is appropriate; if so, whether a secrecy provision is appropriate as part of the scheme; and if so, whether the form of section 35P is appropriate.

Is an SIO scheme appropriate?

37. An SIO scheme of the kind reflected in Division 4 of Part III is appropriate both from the point of view of ASIO and the public. The width of the anti-terrorism laws is such that little covert use of human sources could occur without a breach of the law. There could be a temptation for ASIO personnel to do ‘whatever it takes’ to secure the nation, which could involve cutting corners or more serious breaches. The controversy over methods of interrogation by various international intelligence agencies is one illustration. Division 4 of Part III provides some clear boundaries and, within those boundaries, provides safeguards against abuse. Authorisation is by the Minister rather than ASIO personnel. Certain illegal conduct, described in section 35K(1)(d) and (e), cannot be authorised (broadly, conduct cannot constitute entrapment, cause death or serious injury, constitute torture, involve the commission of a sexual offence or cause significant loss of or damage to property). There are various reporting and oversight requirements, including that the Director-General of ASIO must notify the IGIS (the IGIS has a specific oversight function27) as soon...

---

27 See Appendix G, which includes an explanation from the IGIS of this oversight role. The IGIS can, in an appropriate case, recommend that an agency compensate a person.
as practicable after an SIO authority is granted, and must give six-monthly reports to the Minister and the IGIS on SIOs that are in force. Those reports must include whether an SIO has caused the death of or serious injury to any person, or involved the commission of a sexual offence against any person, or resulted in loss of or damage to property.

38. During this inquiry, I have had the benefit of private hearings about the practical operation of the SIO scheme. I am satisfied that it is necessary and proportionate to the present threat to security and that the procedures in force (both statutory and administrative) are appropriate safeguards against abuse, which is not to say that the possibility of abuse can be discounted entirely. This scheme protects those authorised to act illegally. That makes unauthorised activity less likely and not defensible if it occurs. This should protect the public from ad hoc illegality, whether or not it is authorised or tolerated by the ASIO hierarchy. It is a significant advance on the pre-existing situation.

Is a secrecy provision appropriate?

39. While there are general secrecy provisions in the ASIO Act, a tailored secrecy provision as part of a self-contained scheme of this kind is not inappropriate, particularly as the process for authorisation goes beyond ASIO personnel.

Is section 35P an appropriate secrecy provision?

40. The justification for section 35P in the Explanatory Memorandum to the NSLAB (No 1) 2014 is as follows (emphasis added, a fuller extract of the explanation of section 35P is set out in Appendix B28):

569. New section 35P creates two offences in relation to the unauthorised disclosure of information relating to an SIO. These offences are necessary to protect persons participating in an SIO and to ensure the integrity of operations, by creating a deterrent to unauthorised disclosures, which may place at risk the safety of participants or the effective conduct of the operation.

... 

573. The offence in subsection (1) does not require proof of intent to cause harm, or any proof of resultant harm from the disclosure. This is because the wrongdoing to which it is directed is the harm inherent in the disclosure of adversely affected by the agency’s action, in accordance with section 22 of the Inspector-General of Intelligence and Security Act 1986.

28 See also the emphasised extract of paragraph 3.98 of the PJCIS Report in Appendix B.
highly sensitive intelligence information. The disclosure of the very existence of an SIO—which is intended to remain covert—is, by its very nature, likely to cause harm to security interests. Given the necessarily covert nature of SIOs, disclosure of the existence of such an operation automatically creates a significant risk that the operation may be frustrated or compromised, and that the safety of its participants or persons associated with them, such as family members, may be jeopardised. Once such information is disclosed, there is limited recourse available to address these significant risks. This harm is not contingent on a person’s malicious intention in making a disclosure, except that it may be aggravated by any such malice. As such, the offence in subsection (1) gives effect to the strong need for a deterrent to such behaviour.

41. My examination of the operation of the SIO scheme in practice confirms that risks of the kind outlined are real in relation to certain (perhaps most) kinds of intelligence operations with certain (perhaps most) kinds of authorised illegal behaviour. It does not follow that the same risks will be inherent in relation to all information relating to all SIOs for all time. The rationale for the width of the section depends on harm, of the kind outlined, being implicit in any disclosure of any information about an SIO at any time. That is simply not sustainable. It may be accepted that information about an SIO may seem innocuous, but may be significant if combined with other information that is known: the ‘mosaic’ effect. That does not deny that some information about an SIO will have no, or no continuing, operational significance. It is one thing to enforce an implication of harm in relation to insiders bound by a duty of confidence and with knowledge (or the means of knowledge) about an SIO. It is quite another to apply that implication to third parties who are not so bound and who do not have such knowledge.

42. The fundamental question is whether third parties should be bound by the broad prohibitions of external disclosures effected by section 35P in the same way as insiders (assuming ‘disclose’ has the wide meaning contended by the authorities). The section makes no distinction, either in culpability or penalty. There is no ‘harm’ requirement in the basic offence. That is contrary to the reasoned position of the ALRC, the Gibbs Committee and the Commission of Inquiry into ASIS. 29 For example, the Gibbs Committee recommended that, in the case of a disclosure relating to the intelligence and security services, the

29 See Appendix L, which describes the history of Commonwealth secrecy offences relevant for present purposes.
prosecution would not have to prove damage, but would have to prove damage if the disclosure was made by a person who was not a member or ex-member of those services. In the latter regard, the Gibbs Committee stated:

31.25 Undoubtedly, a member of the intelligence and security services stands in a special position and it is not unreasonable, in the opinion of the Review Committee, that he or she should be subject to a lifelong duty of secrecy as regards information obtained by virtue of his or her position. Subject to the very important proviso that satisfactory procedures are established by which complaints or allegations by such a person as to illegality, misconduct or improper activities of those services or persons employed in them are received, investigated and dealt with (see Chapter 32), the Review Committee is satisfied that disclosures by such persons should be prohibited by criminal sanctions without proof of harm.

43. The principal differences between insiders and outsiders lie in the means of knowledge about an SIO and the obligations of confidentiality owed by insiders. An outsider has no direct means of knowledge and owes no duty of confidence. Unless good cause is shown, it is not acceptable that an outsider, without any duty of confidentiality, should have to risk criminal conviction for publication made without any or any reliable knowledge of the existence or nature of an SIO.

Conclusion—flaws with section 35P and recommended solution

44. I am not satisfied that section 35P contains adequate safeguards for protecting the rights of individuals or that it is proportionate to the threat of terrorism or the threat to national security. Furthermore, for reasons discussed in Appendix J, there are arguments of substance that the impact on journalists of section 35P as it stands infringes the constitutional protection of freedom of political communication and is inconsistent with article 19 of the *International Covenant on Civil and Political Rights*. Three basic flaws need to be addressed. The first is the absence of an express harm requirement for breach (of the basic offence) by a journalist or other third party. The second is that recklessness is the fault element in relation to the circumstance described in section 35P(2)(c)(ii) (that is, in relation to the latter harm requirement in the aggravated offence). The third is the prohibition of disclosure of information already in the public domain.
Harm requirement

45. A prohibition applicable to third parties would properly be directed to the risks that are identified in the passages of the Explanatory Memorandum set out in paragraph 40 above and adopted by the PJCIS in its *Advisory Report on the National Security Legislation Amendment Bill (No 1) 2014* (paragraph 3.98, extracted in Appendix B) as follows:

The Committee considers that to ensure the success of highly sensitive operations and to protect the identity of individuals involved, it is essential that information on these operations not be disclosed.

These risks are reflected in section 35P(2)(c)(ii), which picks up danger to persons and prejudice to the operation from the disclosure.

46. Section 35P should be redrafted to treat insiders and outsiders separately, with one part dealing with third parties and another part dealing with insiders. There should be a basic offence (penalty five years imprisonment) and an aggravated offence (penalty 10 years imprisonment) in relation to both insiders and outsiders.

**Insiders**
The basic offence and the aggravated offences for insiders would be as per current section 35P.

**Outsiders**
The basic offence for outsiders would have the same elements as section 35P(1), but with the additional physical element that the disclosure of the information will endanger the health or safety of any person or prejudice the effective conduct of an SIO. Recklessness would be the default fault element in relation to this last physical element.

The aggravated offence for outsiders would have the same elements as section 35P(2) except that the fault element for (c)(ii) should be knowledge rather than recklessness (in other words, the fault element for the circumstance that the disclosure will endanger the health or safety of any person or prejudice the effective conduct of the operation should be specified to be knowledge).[^30] This difference in approach in relation to outsiders recognises that outsiders have no direct means of knowledge and generally

[^30]: This would enable disclosures that do not risk harm, including sensible consultations prior to publication.
owe no duty of confidence. In my view, this means that recklessness is not an appropriate fault element for an offence with such a significant penalty. However, this recommended approach adopts the same basic structure as section 35P(2).

**Disclosure of information that is in the public domain**

47. There is no particular reason to distinguish information about SIOs from other information as far as ASIO insiders are concerned. No public domain defence is available and this report does not concern insiders. The position of outsiders such as journalists is different. Imposing criminal liability for republishing something already in the public domain needs to be justified. A broad prohibition in the present terms of section 35P could hardly be justified. There is a strong case for providing a public domain defence for outsiders. Different considerations would apply if section 35P was amended to include a harm element as recommended. Section 92 partly overlaps the substance of section 35P(2)(c)(ii) and the prohibition on publication effected by section 92 will remain. On the one hand, publication of information already published might increase dissemination of the harmful material beyond the initial reach and so cause additional harm. On the other hand, the interference with freedom of expression by a permanent ban on discussion of material in the public domain relating to authorised illegal activity is serious and, in the digital age, almost impossible to police.

48. If section 35P is otherwise amended as recommended, it would strike the proper balance to protect journalists (and others) by adopting the substance of the Gibbs Committee recommendation (at 35.1) as follows:

- There should be a defence of prior publication (not available to a member or ex-member of the intelligence and security services in respect of information available to him or her in that capacity), which would require the defendant to satisfy the court:
  - that the information in question had previously been published
  - that, having regard to the nature and extent of that prior publication and the place where it occurred, the defendant had reasonable grounds to believe that the second publication was not damaging, and
  - the defendant was not in any way directly or indirectly involved in the prior publication.
Disclosure of modus operandi

49. Disclosure of an operational capability, method or plan of ASIO (compare section 34ZS) has the potential to harm ASIO operations. This harm was not relied on to justify section 35P in the critical part of the Explanatory Memorandum to the National Security Legislation Amendment Bill (No 1) 2014 or by the PJCIS. It is not reflected in the aggravated offence in section 35P(2) beyond the effect on the SIO in question.\(^{31}\) The broad prohibition of external disclosure of information by ASIO insiders, by administrative means including contract and by legislation,\(^{32}\) is the frontline protection against this harm. This was the situation until section 35P came into force. The introduction of the SIO scheme, authorising illegal behaviour, is not a convincing justification for now prohibiting in the same manner third party publication of such information. This class of harm would cast a wide net of uncertain dimension. If a different view prevailed, the fact that much about the operational capabilities, methods and plans of intelligence organisations (including ASIO) is in the public domain would need to be taken into account, and an appropriate defence would need to be provided.

A public interest defence?

50. A public interest defence in various forms for journalists (and others) was proposed by many, but opposed by ASIO. Such a defence was recommended by the Commission of Inquiry into ASIS but not by the Gibbs Committee or the ALRC.

51. This report deals with limited aspects of the operations of ASIO—it would not be appropriate to depart from the broad prohibition of external disclosure by ASIO insiders in these circumstances. However, the treatment of outsiders requires close examination.

52. A more closely targeted prohibition such as that recommended might still, to some extent, inhibit the exposure of wrongdoing or other aspects of the public interest in relation to an SIO. An example would be complaints about the conduct of the SIO or those involved in the SIO. ASIO and its operations have previously been carefully excluded from, or subjected to limited, public

\(^{31}\) Nor was it relied upon in official comments about the relevant Crimes Act sections – see Appendix M.

\(^{32}\) In particular, sections 18–18B, 34ZS and 92 of the ASIO Act, as well as section 35P.
External scrutiny of ASIO operations was most recently considered by the Parliament in relation to the *Public Interest Disclosure Act 2013*. The prohibition of external disclosure of intelligence information by insiders was maintained. Criticism was answered by pointing out that the IGIS has the function of dealing with complaints (from any source) concerning intelligence agencies and intelligence information. That would include complaints relating to an SIO. A number of submissions to this inquiry did not see that remedy as a satisfactory solution. In particular, the IGIS is seen by some as part of the security and intelligence establishment, as having limited functions and resources and bound to maintain secrecy.

53. There is a case for a public interest defence for journalists (and others) as section 35P currently stands, notwithstanding the difficulty for the prosecution of establishing recklessness and the discretions of the Attorney-General and the CDPP in relation to prosecutions, as discussed earlier. The addition of the recommended element of harm to the basic offence changes the equation. The publication of harmful material would be properly prohibited. Any special circumstances can be taken into account in decision making by the Attorney-General and the CDPP (and, potentially, in relation to sentencing). The judiciary should not lightly be involved in binding value judgments about issues of national security. The case for doing so is not sufficient if section 35P is amended as recommended.

**A lack of knowledge defence?**

54. The Gibbs Committee recommended:

(g) It should be a defence for a person charged with an offence under the proposed provisions where proof of damage is required that he or she did not know and had no reasonable cause to believe that the information related to the matters in question or that its disclosure would be damaging.

Such a defence should not be necessary where the onus is on the prosecution to establish recklessness in relation to relevant matters.

---

33 Appendix I describes some aspects of the public accountability of ASIO and its operations.
34 See Appendix G, which contains some relevant comments and an extract from the IGIS submission to this inquiry. The IGIS *Annual Report 2014-2015* states (at page 4) “It is difficult for the office to continue to demonstrate rigorous and credible oversight given the strict limitations on public reporting”.

---
Sunset provision

55. If the recommended amendments are adopted there should be no need for a sunset clause. Further experience of section 35P will continue to be subject to INSLM review.

Conclusion

56. If these recommendations are implemented, an SIO would be protected by wider secrecy provisions than other covert ASIO operations. However, freedom of expression would be inhibited only to a reasonable minimum—proportionate to the threat, including of terrorism, to national security and consistent with constitutional imperatives and Australia’s international human rights obligations. There would also be appropriate safeguards for protecting the rights of individuals.
Appendix A—List of contributors to the inquiry

The inquiry received public submissions from (in order of receipt):

- Seven West Media (Seven Network, Pacific Magazines, Yahoo7 and the West Australian and other Western Australian newspapers and radio stations)/Addisons Lawyers, for Seven West Media
- National tertiary Education Union
- Gilbert + Tobin Centre of Public Law, University of New South Wales
- Professor Emeritus Clive Walker, University of Leeds
- Professor Jason Sharman, Griffith University
- Professor Rick Sarre, University of South Australia
- Civil Liberties Australia
- Attorney-General’s Department and the Australian Security Intelligence Organisation (including in response to requests for information)
- Dr Matt Collins QC
- Senator Nick Xenophon and Dr Clinton Fernandes, University of New South Wales at the Australian Defence Force Academy
- Marque Lawyers
- Bar Association of Queensland
- Law Council of Australia
- Australian Lawyers for Human Rights
- Acting Professor Margaret Simons and Gary Dickson, Centre for Advancing Journalism, University of Melbourne
- Amnesty International
- Professor Russell Trood and Kate Grayson, Griffith University
- Commonwealth Director of Public Prosecutions (including in response to requests for information)
- Human Rights Watch

---

35 Two submissions listed on the INSLM website were responses by AGD and ASIO respectively to requests for information. Two confidential written submissions were also received.
Chris Berg and Simon Breheny, Institute of Public Affairs
Australian Federal Police, in response to a request for information
Councils for Civil Liberties (Australian, New South Wales, Victorian, Queensland and South Australian)
Australian Human Rights Commission
New South Wales Bar Association
Guardian Australia
Tasmanian Government, in response to a request for information
Law Society of New South Wales
Premier of Queensland, in response to a request for information
Chief Minister, Northern Territory Government, in response to a request for information
Premier of South Australia, in response to a request for information
Faculty of Law, Bond University
Inspector-General of Intelligence and Security
Victorian Government, in response to a request for information
Humanist Society of Victoria
New South Wales Government, in response to a request for information
Chief Minister, Australian Capital Territory, in response to a request for information.

The INSLM held public hearings on 27 and 28 April 2015 and met with the following people and groups:

- Joint Media Organisations
  - Adam Suckling, Director—Policy, Corporate Affairs and Community Relations, News Corp Australia
  - Campbell Reid, Group Editorial Director, News Corp Australia
  - Paul Murphy, CEO, Media Entertainment and Arts Alliance
Georgia-Kate Schubert, Head of Police and Government Affairs, News Corp Australia

Bridget Fair, Group Chief, Corporate and Regulatory Affairs Seven West Media

Senator Nick Xenophon

Dr Clinton Fernandes, University of New South Wales at the Australian Defence Force Academy

Law Council of Australia
  – Stephen Keim SC, National Human Rights Committee
  – Matthew Dunn, Director of Policy
  – Dr Natasha Molt, Senior Policy Adviser

Michael Bradley, Managing Partner, Marque Lawyers

Laura Thomas, Human Rights Watch Australia Committee

Dr Lesley Lynch, for Councils for Civil Liberties

Civil Liberties Australia
  – Dr Kristine Klugman, President
  – Bill Rowlings, CEO

Dr Paul Kniest, Policy and Research Coordinator, National Tertiary Education Union

Gilbert + Tobin Centre of Public Law (via teleconference)
  – Professor George Williams AO
  – Dr Keiran Hardy

Attorney-General’s Department
  – Jamie Lowe, First Assistant Secretary, National Security Law and Policy Division
  – Julie Taylor, acting National Security Legal Adviser

Australian Federal Police
  – Acting Commissioner, Michael Phelan
  – Commander Peter Crozier, performing duties of National Manager Counter Terrorism

Australian Security Intelligence Organisation
  – Duncan Lewis AO DSC CSC, Director-General of Security
  – Kerri Hartland, Deputy Director-General
• Commonwealth Director of Public Prosecutions
  – Scott Bruckard, Deputy Director, Organised Crime and Counter-Terrorism
  – Stefanie Cordina, Principal Federal Prosecutor, Organised Crime and Counter-Terrorism.

The INSLM also held private hearings with the:

• Australian Security Intelligence Organisation
• Australian Federal Police
• Commonwealth Director of Public Prosecutions
• Inspector-General of Intelligence and Security.
Appendix B—Legislative history of section 35P

Parliamentary Joint Committee on Intelligence and Security report 2013

During 2012, the then Australian Government asked the Parliamentary Joint Committee on Intelligence and Security (PJCIS) to inquire and report on a range of potential reforms to national security legislation.

The Attorney-General’s Department (AGD) and agencies within the Australian Intelligence Community (AIC) had identified a number of practical difficulties with the legislation governing the operations of those agencies.

The Government identified:

- proposals the Government wished to progress
- matters the Government was considering (including amending the ASIO Act to create an authorised intelligence operations scheme), and
- matters on which the Government was seeking the views of the PJCIS.

In July 2012 the PJCIS issued the Discussion Paper, *Equipping Australia against emerging and evolving threats*. The following section of the Discussion Paper dealt with an authorised intelligence operations scheme:

3. Matters the Government is considering

3.1 Amend the ASIO Act to create an authorised intelligence operations scheme

ASIO’s continued ability to collect useful and relevant intelligence on the most serious threats to the security of Australia and Australians, hinges on its capacity to covertly gain and maintain close access to highly sensitive information. This activity often involves engaging and associating closely with those who may be involved in criminal activity and therefore has the potential to expose an ASIO officer or human source to criminal or civil liability, in the course of their work.

With the enactment of broad overarching laws criminalising security related issues, many of those targets under investigation are involved in activities that breach the criminal law. Increasingly, those laws are capable of capturing the activities of persons who are associating covertly with targets, notwithstanding that their activities are for lawful intelligence collection purposes.

For example, under Part 5.3 of the Criminal Code, it is an offence to intentionally provide training to or receive training from a terrorist organisation where the person
is reckless as to whether the organisation is a terrorist organisation. Therefore, if an
ASIO officer or human source is tasked to collect covert intelligence in relation to a
terrorist organisation, they may be open to criminal liability under the Criminal Code
if, in the course of collecting the relevant intelligence, they receive training from that
organisation.

An authorised intelligence operations scheme would significantly assist covert
intelligence operations that require undercover ASIO officers or human sources to
gain and maintain access to highly sensitive information concerning serious threats
to Australia and its citizens. A scheme similar to the controlled operations scheme
under the Crimes Act 1914 could be developed to apply to ASIO officers and human
sources operating under the ASIO Act, with appropriate modifications and
safeguards that recognise the scheme would operate in the context of covert
intelligence gathering investigations or operations.

Should an authorised intelligence operations regime be pursued, it will be critical
that it achieves an appropriate balance between operational flexibility and
appropriate oversight and accountability. Key features that may contribute to such
could include:

• the Director-General of Security to issue authorised intelligence operation
certificates which would provide protection from criminal and civil liability
for specified conduct for a specified period (such as 12 months)
• oversight and inspection by the Inspector-General of Intelligence and
Security (IGIS), including notifying the IGIS once an authorised intelligence
operation has been approved by the Director-General
• specifying conduct which cannot be authorised (e.g., intentionally inducing
a person to commit a criminal offence that the person would not otherwise
have intended to commit and conduct that is likely to cause the death of or
serious injury to a person or involves the commission of a sexual offence
against any person), and
• independent review of the operation, effectiveness and implications of any
such scheme, which could be conducted five years after the scheme’s
commencement.

Legislation, dated May 2013, was tabled in Parliament on 24 June 2013. The report
includes the following relevant comment and recommendation:

Committee comment

4.116 The Committee received evidence that there are occasions on which ASIO
officers and sources are placed in positions where, in order to carry out
their duties, they may need to engage in conduct which may, in ordinary
circumstances, be a breach of the criminal law. The Committee
understands that such occasions would be seldom but may from time to time arise. The Committee also understands that it will not be possible for ASIO to rely on the existing framework under which the AFP operates.

4.117 The Committee is therefore of the view that the ASIO Act should be amended to create a controlled intelligence operations scheme.

4.118 The discussion paper suggests particular restrictions, reporting and accountability mechanisms. The Committee agrees that an ASIO authorised intelligence operations scheme should be subject to strict accountability and oversight.

4.119 The Committee supports the adaptation of the procedures and safeguards in the Crimes Act 1914 that apply to the AFP’s controlled operations. This would mean that ASIO officers and agents would be exempted from criminal and civil liability only for certain authorised conduct.

4.120 The Committee expects that unreasonable or reckless conduct would not be indemnified by an authorised intelligence operation, and the ASIO officer or source would be liable for such conduct.

Recommendation 28

The Committee recommends that the Australian Security Intelligence Organisation Act 1979 be amended to create an authorised intelligence operations scheme, subject to similar safeguards and accountability arrangements as apply to the Australian Federal Police controlled operations regime under the Crimes Act 1914.

National Security Legislation Amendment Bill (No 1) 2014 introduced into the Senate

The Australian Government introduced the National Security Legislation Amendment Bill (No 1) 2014 (NSLAB (No 1) 2014) into the Senate on 16 July 2014. Section 35P of the Bill was expressed in the following terms:

35P Unauthorised disclosure of information

Unauthorised disclosure of information

(1) A person commits an offence if:
   (a) the person discloses information; and
   (b) the information relates to a special intelligence operation.

Penalty: Imprisonment for 5 years.
Unauthorised disclosure of information—endangering safety, etc.

(2) A person commits an offence if:
   (a) the person discloses information; and
   (b) the information relates to a special intelligence operation; and
   (c) either:
      (i) the person intends to endanger the health or safety of any person
          or prejudice the effective conduct of a special intelligence
          operation; or
      (ii) the disclosure of the information will endanger the health or
           safety of any person or prejudice the effective conduct of a
           special intelligence operation.

Penalty: Imprisonment for 10 years.

Exceptions

(3) Subsections (1) and (2) do not apply if the disclosure was:
   (a) in connection with the administration or execution of this Division; or
   (b) for the purposes of any legal proceedings arising out of or otherwise
       related to this Division or of any report of any such proceedings; or
   (c) in accordance with any requirement imposed by law; or
   (d) in connection with the performance of functions or duties, or the
       exercise of powers, of the Organisation.

Note: A defendant bears an evidential burden in relation to the matters in this subsection—see subsection 13.3(3) of the Criminal Code.

Extended geographical jurisdiction

(4) Section 15.4 of the Criminal Code (extended geographical jurisdiction—category D) applies to an offence against subsection (1) or (2).

(5) Subsection (4) does not, by implication, affect the interpretation of any other provision of this Act.

The NSLAB (No 1) 2014 implemented the Government’s response to the recommendations in Chapter 4 of the 2013 PJCIS report (including recommendation 28).

The Attorney-General immediately referred the NSLAB (No 1) 2014 to the PJCIS for inquiry and report by 17 September 2014.

PJCIS Report on the NSLAB (No 1) 2014 tabled in Parliament

The following extracts from the report relate to the SIO scheme. They relate to the scheme as a whole, not just proposed section 35P. They are included because they provide a useful explanation of the statutory context of section 35P. (The extracts are from Chapter 2, following an outline of the previously proposed scheme and previous recommendation 28; and from Chapter 3, comment and recommendations, with footnotes omitted.)

2.51 The Bill proposes to implement this recommendation by introducing into the ASIO Act a statutory framework for the conduct of ‘special intelligence operations’ (SIOs). The SIO scheme is ‘based broadly’ on the controlled operations scheme in the Crimes Act 1914, although ‘appropriate modifications have been made to reflect the differences between a law enforcement operation … and a covert intelligence-gathering operation’.

2.52 The intent of the scheme is to ‘ensure ASIO officers, employees and agents will have appropriate legal protections when conducting covert operations’, for example, if an ASIO officer were to attend, as part of a covert operation, a training session provided by a terrorist organisation. The Explanatory Memorandum notes that ‘at present, some significant covert operations either do not commence or are ceased due to the risk that participants could be exposed to criminal or civil liability’.

2.53 The commencement of an SIO would be subject to authorisation by the Director-General or Deputy Director General of Security. Authorisation of an SIO would be subject to criteria outlined in proposed section 35C, including that any unlawful conduct under the SIO would be ‘limited to the maximum extent’ and would not include causing death or serious injury to a person, committing a sexual offence, or causing significant loss or damage to property. The immunity provided under the scheme would be limited to conduct authorised under the SIO (proposed section 35K). Further, proposed section 35L stipulates that conduct authorised under an SIO would not affect the need to obtain a warrant for certain activities under the ASIO Act or Telecommunications (Interception and Access) Act 1979.

2.54 Proposed section 35P creates two offences in relation to unauthorised disclosure of information relating to an SIO. These comprise a basic offence carrying a five year maximum jail term; and an aggravated offence carrying a ten year maximum jail term for cases in which the person endangers, or intends to endanger, the effectiveness of the SIO or the health or safety of those involved. The Explanatory Memorandum makes it clear that these offences could apply to anyone:
The offences apply to disclosures by any person, including participants in an SIO, other persons to whom information about an SIO has been communicated in an official capacity, and persons who are the recipients of an unauthorised disclosure of information, should they engage in any subsequent disclosure.

2.55 Proposed section 35Q outlines specific reporting requirements for the SIO scheme, comprising six-monthly written reports to the Minister and the IGIS on the extent to which each SIO has assisted ASIO in its functions.

Committee comment

3.89 After considering the matter in its 2013 inquiry, the Committee previously recommended that a controlled intelligence operation scheme be introduced ‘subject to similar safeguards and accountability arrangements as apply to the Australian Federal Police controlled operations regime’. The purpose of this current inquiry is not to reconsider the rationale for such a scheme, but rather to assess the adequacy of the safeguards included in the scheme as it is proposed, including its offence provisions. The Committee notes that, despite its previous recommendation being ‘supported’, not all the safeguards included in the AFP controlled operations regime are included in the SIO scheme proposed in this Bill.

3.90 During the inquiry, the Committee suggested that many of the concerns raised by participants about the potential for misuse, or overuse, of the SIO scheme would be allayed if an independent issuing authority was required to authorise the commencement of any new SIO. The purpose of such a model would be to lessen the perceived risk of SIO powers being used for purposes beyond those envisaged in the Bill, and through this, strengthening public confidence in the integrity of the scheme.

3.91 Nonetheless, the Committee is conscious that any alternative authorisation model should not impede ASIO’s operational requirements to initiate SIOs in a timely and considered manner. The Committee accepts the Attorney-General’s Department and ASIO’s reservations that an external authorisation model may impede timely and effective operations.

3.92 The Committee considers that the alternative proposal by the Department and ASIO for additional requirements around notifications and reporting would significantly enhance the IGIS’s (and Attorney-General’s) oversight of the SIO regime. In particular, the proposals would enhance the ability of the IGIS to oversee the commencement of new SIOs
and to assess any potential need for compensation due to injury, loss or damage to persons or property.

3.93 The Committee also considers that the suggested requirement for the IGIS to periodically inspect the records of current SIOs would be effective in encouraging sustained, close scrutiny of the scheme’s operation into the future. The Committee encourages the IGIS to pay particularly close attention to decisions to authorise the commencement or variation of each SIO to ensure their ongoing compatibility with the stated intent of the scheme.

3.94 While these proposals are helpful and will strengthen oversight of the SIO regime by the IGIS, the Committee is not convinced that retrospective oversight is sufficient given the seriousness of action that could be taken under an SIO and the necessary lack of public transparency over those actions. The Committee considers that an additional level of authorisation should be required to be obtained by ASIO before an SIO can commence. Taking into account concerns about the operational impact of an external authorisation regime, and also the need for sufficient oversight and accountability, the Committee is of the view that authorising approval from the Attorney-General should be a requirement of an SIO.

3.95 The Committee therefore makes the following two recommendations to strengthen the integrity of oversight requirements for the SIO scheme:

Recommendation 9

The Committee recommends that Schedule 3 to the National Security Legislation Amendment Bill (No. 1) 2014 be amended to require that approval must be obtained from the Attorney-General before a special intelligence operation is commenced, varied or extended beyond six months by the Australian Security Intelligence Organisation.

Recommendation 10

The Committee recommends that additional requirements be introduced into the National Security Legislation Amendment Bill (No. 1) 2014 to enhance the Inspector-General for Intelligence and Security (IGIS)’s oversight of the proposed Special Intelligence Operations scheme, including:

- a requirement for the Australian Security Intelligence Organisation (ASIO) to notify the IGIS when a special intelligence operation is approved
- a requirement for ASIO to advise the IGIS of any special intelligence operation that is intended to continue beyond six months
• a requirement for ASIO to notify the Attorney-General and the IGIS, as part of the six-monthly reports proposed in clause 35Q of the Bill, of any injury, loss or damage caused to a person or property in the course of a special intelligence operation, and

• a requirement for the IGIS to periodically, and at least annually, inspect ASIO’s records relating to current special intelligence operations.

3.96 As SIOs are expected to be used only in the most highly sensitive circumstances, the Committee accepts the need for specific offence provisions to confer a higher level of protection for information about SIOs than for other operational matters. The Committee notes that the specific offence provisions contained in proposed section 35P of the Bill were modelled on similar provisions contained in the Crimes Act 1914 for law enforcement controlled operations.

3.97 The Committee appreciates the Department’s efforts to directly and comprehensively respond to concerns raised by inquiry participants about the offence provisions in the proposed SIO scheme.

3.98 The Committee paid close attention to concerns raised by inquiry participants about the potential impact of the proposed offences on press freedom. The Committee considers that in order to ensure the success of highly sensitive operations and to protect the identity of individuals involved, it is essential that information on these operations not be disclosed.

3.99 However, the Committee also considers that it is important for this need for secrecy not to penalise legitimate public reporting. The Committee notes that, under the Criminal Code Act 1995, the fault element of ‘recklessness’ would apply to any prosecution of offences under proposed section 35P. This would mean that to be successful, the prosecution would be required by legislation to prove that a disclosure was ‘reckless’. The structure of the offence provisions, as well as the requirement for the Commonwealth Director of Public Prosecutions to take the public interest into account before initiating a prosecution, provides an appropriate level of protection for press freedoms while balancing national security. However the Committee sees value in making these safeguards explicit in the Bill or the Explanatory Memorandum.

3.100 The Committee considers that these safeguards, coupled with increased oversight by the IGIS over the issuing of SIOs, will provide appropriate protection for individuals, including journalists, who inadvertently make a disclosure of information about a current SIO. The Committee also highlights the important role of ASIO’s existing 24-hour media unit in
providing opportunities for journalists to clarify any concerns about a possible operation, including about the re-publication of any information.

3.101 Taking these safeguards into account, the Committee does not consider it appropriate to provide an explicit exemption for journalists from the proposed offence provisions. Part of the reason for this is that the term ‘journalism’ is increasingly difficult to define as digital technologies have made the publication of material easier. The Committee considers that it would be all too easy for an individual, calling themselves a ‘journalist’, to publish material on a social media page or website that had serious consequences for a sensitive intelligence operation. It is important for the individual who made such a disclosure to be subject to the same laws as any other individual.

3.102 The Committee is, however, concerned to ensure that any unintended consequences of the proposed SIO offence provisions are avoided. As such, the Committee fully supports the Department and ASIO’s suggestion to introduce an explicit exemption from the offences for disclosure of information in the course of obtaining legal advice.

3.103 The Committee also supports explicit exemptions to be introduced for the disclosure of information to the IGIS. To avoid any doubt about the applicability of the PID Act, the Committee considers it should be made explicit in the Bill that this exemption applies to all persons making a complaint to the IGIS, including public officials.

Recommendation 11

The Committee recommends that additional exemptions be included in the offence provisions relating to disclosure of information on special intelligence operations in proposed section 35P of the National Security Legislation Amendment Bill (No. 1) 2014 to explicitly enable

- disclosure of information for the purpose of obtaining legal advice
- disclosure of information by any person in the course of inspections by the Inspector-General of Intelligence and Security (IGIS), or as part of a complaint to the IGIS or other pro-active disclosure made to the IGIS
- communication of information by IGIS staff to the IGIS or other staff within the Office of the IGIS in the course of their duties.
Recommendation 12

The Committee recommends that the National Security Legislation Amendment Bill (No. 1) 2014 be amended or, if not possible, the Explanatory Memorandum of the Bill be clarified, to confirm that the Commonwealth Director of Public Prosecution must take into account the public interest, including the public interest in publication, before initiating a prosecution for the disclosure of a special intelligence operation.

Recommendation 13

The Committee further recommends that, to make clear the limits on potential prosecution for disclosing information about special intelligence operations, Section 35P of the National Security Legislation Amendment Bill (No. 1) 2014 be amended to confirm that the mental element (or intent) of the offence is ‘recklessness’, as defined in the Criminal Code, by describing the application of that mental element to the specific offence created by section 35P.

Scrutiny of the NSLAB (No 1) by the Senate Standing Committee for the Scrutiny of Bills

The NSLAB (No 1) 2014 was also the subject of scrutiny by the Senate Standing Committee for the Scrutiny of Bills. The Committee reported on this subject in the its Twelfth Report of 2014 (24 September 2014). That report included the following comments (pages 627–628) relating to proposed section 35P:

The explanatory memorandum suggests these ‘offences are necessary to protect persons participating in an SIO and to ensure the integrity of operations, by creating a deterrent to unauthorised disclosures, which may place at risk the safety of participants or the effective conduct of the operation’ (at p. 111). The explanatory memorandum also explains that the offences may be committed by any ‘persons to whom information has been [sic] about an SIO has been communicated in an official capacity, and persons who are the recipients of an unauthorised disclosure on [sic] information, should they engage in subsequent disclosure’.

Although the purposes of protecting the integrity of operations and the safety of participants in operations can be readily understood, it must also be noted that these offences are drafted so as to have broad application. First, they are not limited to initial disclosures of information relating to an SIO but cover all subsequent disclosures (even, it would seem, if the information is in the public domain). In addition, these new offences as currently drafted may apply to a wide range of people including whistleblowers and journalists.

Second, the primary offence (unlike the aggravated version) is not tied to the underlying purposes of the criminalisation of disclosure. This means that the offence
(under subsection 35P(1)) could be committed even if unlawful conduct in no way jeopardises the integrity of operations or operatives. The concern about the breadth of application of these offences, in light of their purposes, is arguably heightened given that whether or not the disclosure of information will be caught by the provisions depends on whether or not the information relates to an SIO, a question which depends on an authorisation process which is internal to the Organisation.

As the justification for the breadth of application of these provisions is not directly addressed in the explanatory memorandum the committee seeks a more detailed justification from the Attorney-General in this regard. The committee emphasises that its interest is not only in the underlying purposes served by the provisions, but whether these purposes could be achieved by offences that are more directly connected and proportionate to the achievement of those purposes.

A further reason why these offences may be considered to be too broad in their application is that it is possible they may apply to the disclosure of information even if the person who discloses the information is not aware that it relates to an SIO. Given the nature of an SIO it is likely that only persons within the Organisation will know whether information relates to an SIO. It is also relevant to note that the boundaries of an SIO, and therefore what information ‘relates’ to such an operation, may be unclear to the extent that an SIO authority need only state ‘a general description of the nature of the special intelligence conduct that the persons authorised to engage in conduct for the purposes of the SIO ‘may engage in’ (paragraph 35D(1)(c)). The committee therefore also seeks clarification about (and a justification for) the applicable fault requirement in relation to the element that ‘the information relates to a special intelligence operation’ (paragraph 35P(1)(b) and paragraph 35P(2)(b)).

Pending the Attorney-General’s reply the committee draws Senators’ attention to the provision, as it may be considered to trespass unduly on personal rights and liberties, in breach of principle 1(a)(i) of the committee’s terms of reference.

After including extracts from the Attorney-General’s response and requesting that certain additional information be included in the Explanatory Memorandum, the Committee drew section 35P to the attention of Senators and left the question of whether the proposed approach was appropriate to the Senate as a whole.

The NSLAB (No 1) 2014 passed by the Senate and introduced into the House of Representatives

The NSLAB (No 1) 2014 passed the Senate on 25 September 2014 and was introduced into the House of Representatives on 30 September 2014.

The Second Reading Speech to the NSLAB (No 1) 2014, Hansard, House of Representatives, 1 October 2014, Mr Keenan (Stirling, Minister for Justice)
describes as follows the PJCIS report and the approach taken by the Government to that report and in relation to the SIO scheme:

The committee unanimously recommended that the Bill be passed, subject to the implementation of 16 targeted improvements to improve oversight, accountability and other safeguards. The government accepted all of these suggestions, and moved amendments in the Senate to implement the relevant recommendations. These measures were passed by the Senate on 25 September, and represent valuable improvements to the Bill.

...

The third key reform is the implementation of a recommendation of the Parliamentary Joint Committee on Intelligence and Security in its 2013 inquiry to establish a dedicated statutory framework for ASIO’s covert intelligence-gathering operations.

Much of the intelligence information that is relevant to the security of Australia must necessarily be collected by the organisation on a covert basis.

However, such covert operations are not without risks. In addition to the potential risks to the safety of participants, covert operations can in some instances require participants to associate with those who may be involved in criminal activity—for instance, the commission of offences against the security of the Commonwealth.

Covert operations may, therefore, expose intelligence personnel or sources to legal liability in the course of their work. For this reason, some significant covert operations do not commence or are ceased.

To address this issue, the bill creates a limited immunity for participants in authorised, covert operations.

Just as part IAB of the Crimes Act provides for a limited immunity for covert law enforcement operations, it is appropriate that corresponding protections are extended to participants in covert intelligence operations.

Consistent with the parliamentary joint committee’s recommendations in its 2013 and 2014 inquiries, the limited immunity is subject to rigorous safeguards.

In particular, it is restricted to the conduct of a participant in a special intelligence operation that is authorised by the Attorney-General. The participant and the specific conduct must be authorised expressly in advance. There are a number of reporting requirements to the Attorney-General and the Inspector-General of Intelligence and Security, where an operation is commenced, periodically every six months, and where certain conduct is engaged in (namely that which causes death, serious injury or property damage).
As an additional safeguard, the limited immunity from legal liability expressly excludes conduct in the nature of entrapment, serious offences against the person or property, and torture.

**The NSLAB (No 1) 2014 passed by the House of Representatives**

The NSLAB (No 1) 2014 passed the House of Representatives on 1 October 2014 and received Royal Assent on 2 October 2014.

**Proposed amendments of the NSLAB (No 1) 2014 rejected by the Parliament**

Non-government Members of Parliament in each House of Parliament moved a number of proposed amendments to the Bill. Aside from proposed amendments moved by the Government in the Senate and forming part of the Bill considered by the House of Representatives, the proposed amendments relating to the SIO scheme were rejected by the Parliament.

The rejected proposed amendments relating to section 35P are summarised below:

- that subsection 35P(1) be omitted from the Bill
- that a court determining a sentence for an offence against subsection 35P(1) be required to take account of whether or not, to the knowledge of the court, the disclosure was in the public interest
- that subsection 35P(2) omit reference to prejudice to the effective conduct of an SIO (ie, that the aggravating aspects of the offence be limited to endangering the safety of any person)
- that there be additional exceptions to the offences for a disclosure:
  - of information that has already been disclosed by the Minister, the Director-General or a Deputy Director-General, or
  - made reasonably and in good faith and in the public interest
- that there be an additional exception where:
  - the person has informed ASIO about the proposed disclosure at least 24 hours before making the disclosure and
  - the disclosure did not include information on the identities of participants of an SIO or on a current SIO, and
  - the information concerns corruption or misconduct in relation to an SIO.
Relevant extracts from the Explanatory Memorandum to the NSLAB (No 1) 2014

The Notes on Clauses part of the Explanatory Memorandum to the NSLAB (No 1) 2014 provides the following explanation of section 35P:

**New section 35P—Unauthorised disclosure of information**

569. New section 35P creates two offences in relation to the unauthorised disclosure of information relating to an SIO. These offences are necessary to protect persons participating in an SIO and to ensure the integrity of operations, by creating a deterrent to unauthorised disclosures, which may place at risk the safety of participants or the effective conduct of the operation.

570. The offences apply to disclosures by any person, including participants in an SIO, other persons to whom information about an SIO has been communicated in an official capacity, and persons who are the recipients of an unauthorised disclosure of information, should they engage in any subsequent disclosure.

571. The term ‘disclose’ is intended to take its ordinary meaning for the purpose of section 35P. It is intended to include the making available of information to others by any means. It is not intended to require, as a rule, proof that the information was received by another person, or proof that another person read, heard or viewed the information. Nor is the term intended to require proof that a person provided or intended to provide information to a particular person or group of persons.

**Offence of unauthorised disclosure of information relating to an SIO—new subsection 35P(1)**

572. New subsection 35P(1) creates an offence applying to the conduct of a person in the form of a disclosure of information, and a circumstance that the information relates to an SIO. The fault element of intention applies to the physical element of a person’s conduct in disclosing information, by reason of subsection 5.6(1) of the Criminal Code. The fault element of recklessness applies to the physical element of the circumstance that the information relates to an SIO, by reason of subsection 5.6(2) of the Criminal Code. The offence carries a maximum penalty of five years’ imprisonment. This is confirmed by a note to subsection (1), which was inserted following recommendation 13 of the Parliamentary Joint Committee on Intelligence and Security in its inquiry into the Bill. The note has been included to acknowledge the Committee’s concern to ensure that the significant threshold imposed by the fault element of
recklessness is communicated expressly on the face of the provisions, in recognition of concerns raised in the course of the Committee’s inquiry. It does not displace the general principles of criminal responsibility in Chapter 2 of the Criminal Code, which are of general application to all Commonwealth offences and are not required to be expressly stated in individual offence provisions. The insertion of a purely declaratory note to this effect is an exceptional measure.

573. The offence in subsection (1) does not require proof of intent to cause harm, or any proof of resultant harm from the disclosure. This is because the wrongdoing to which it is directed is the harm inherent in the disclosure of highly sensitive intelligence information. The disclosure of the very existence of an SIO—which is intended to remain covert—is, by its very nature, likely to cause harm to security interests. Given the necessarily covert nature of SIOs, disclosure of the existence of such an operation automatically creates a significant risk that the operation may be frustrated or compromised, and that the safety of its participants or persons associated with them, such as family members, may be jeopardised. Once such information is disclosed, there is limited recourse available to address these significant risks. This harm is not contingent on a person’s malicious intention in making a disclosure, except that it may be aggravated by any such malice. As such, the offence in subsection (1) gives effect to the strong need for a deterrent to such behaviour.

574. The maximum penalty of five years’ imprisonment reflects that a person was reckless in making the disclosure, and maintains parity with the penalties applying to the secrecy offences in s 34ZS of the ASIO Act, concerning the unauthorised disclosure of information relating to ASIO’s questioning and detention warrants. These offences similarly do not require proof of intent to cause harm or resultant harm, in recognition that such harm is implicit in the sensitive nature of the information.

*Aggravated offence—new subsection 35P(2)*

575. New subsection 35P(2) creates an aggravated form of the offence in subsection 1. The relevant aggravating elements, which are set out in paragraph (c), are that:

(i) the person intended, in making the disclosure, to endanger the health or safety of any person, or prejudice the effective conduct of an SIO, or

(ii) the disclosure of the information will endanger the health or safety of any person or prejudice the effective conduct of an SIO.
576. The fault element applying to the physical element in paragraph 35P(2)(c)(i) is that of intention, pursuant to the express statement in the provision. The fault element applying to the physical element in paragraph 35P(2)(c)(ii) is that of recklessness, by reason of subsection 5.6(2) of the Criminal Code. The aggravated offence is subject to a maximum penalty of 10 years’ imprisonment. The note to subsection (2) is in identical terms to that in subsection (1) and has been included for the same reasons (as outlined above).

Offence-specific defence—new subsection 35P(3)

577. The new offences in subsections 35P(1) and (2) are subject to an offence-specific defence in subsection 35P(3), which provides for a number of lawful disclosures in paragraphs 35P(3)(a)-(g). These include disclosures pertaining to the operation of Division 4 or legal proceedings relating to Division 4, other legal obligations of disclosure, the performance by the Organisation of its statutory functions, obtaining legal advice in relation to the SIO, disclosures to an IGIS official for the purpose of the IGIS exercising powers or performing functions or duties under the IGIS Act, and disclosures by an IGIS official in connection with the IGIS official exercising such powers or performing such functions or duties.

578. The exceptions in favour of legal advice, and disclosures to or by IGIS officials in paragraphs (e)–(g) implement recommendation 11 of the Parliamentary Joint Committee on Intelligence and Security. The Committee was concerned to ensure that an exception was available for the provision of legal advice in circumstances in which proceedings were not commenced in relation to an SIO. The Committee was further concerned to ensure that the offences in section 35P did not operate as a perceived disincentive to the communication of information to the IGIS in connection with his or her statutory oversight functions.

579. Consistent with subsection 13.3(3) of the Criminal Code, the defendant bears an evidential burden in relation to the offence-specific defence in subsection 35P(3). This means that he or she must adduce or point to evidence suggesting a reasonable possibility that one or more of the matters set out in paragraphs 35P(3)(a)-(g) exist. The prosecution is then required to negate this matter to the legal standard (beyond reasonable doubt).

580. It is appropriate to frame the matters in subsection 35P(3) as an offence-specific defence (with the result that an evidential burden is imposed on the defendant) rather than including these matters as an element of the offences in subsections 35P(1) and (2). For example, a requirement that
the disclosure was not made pursuant to any of the matters set out in paragraphs 35P(3)(a)-(g), with the result that the prosecution bears the legal and evidential burden.

581. This is because evidence suggesting a reasonable possibility of the authorised nature of the disclosure is readily available to a defendant, who would have had such authority, or perceived authority, in contemplation at the time he or she disclosed the relevant information. The inclusion of subsection 35P(3) as an element of the offences in subsections 35P(1) and (2) would be inappropriate is it would impose a disproportionate burden on the prosecution. It would be necessary for the prosecution to disprove, as a matter of course, all of the matters set out in paragraphs 35P(3)(a)–(g) even if there is no evidence suggesting they are in issue.

582. Subsection 35P(3) does not include an express defence for the communication of information relating to a special intelligence operation, where such communication is found to be in the public interest. The Commonwealth Director of Public Prosecutions (CDPP) is required, under the Prosecution Policy of the Commonwealth, to consider the public interest in the commencement or continuation of a prosecution. It would be open to the CDPP, in making independent decisions on this matter, to have regard to any public interest in the communication of information in particular instances as the CDPP considers appropriate.

Penalties

583. The penalties applying to these offences implement a gradation consistent with established principles of Commonwealth criminal law policy, as documented in the Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers. The Guide provides that a heavier maximum penalty is appropriate where the consequences of an offence are particularly dangerous or damaging.

584. The offence in subsection 35P(2), applying to the disclosure of information with an intent to cause harm (or where harm will result from such a disclosure), appropriately attracts a heavier penalty than the offence in subsection 35P(1), which targets conduct that places at risk such information. The penalty of 10 years’ imprisonment applying to the aggravated offence in subsection 35P(2) maintains parity with the penalty applying to the offence of unauthorised communication of information in subsection 18(2) (as that penalty is amended by Schedule 6).

585. The maximum penalty of five years’ imprisonment applying to the offence in subsection (1) reflects an appropriate gradation with the new
unauthorised dealing offences in sections 18A and 18B (inserted by Schedule 6) which carry a maximum penalty of three years’ imprisonment, and parity with section 34ZS of the ASIO Act regarding the unauthorised disclosure of information relating to a questioning or questioning and detention warrant. The unauthorised disclosure of information pertaining to an SIO is considered to be more culpable than the unauthorised dealing with information pertaining to the Organisation’s statutory functions. For example, the unauthorised disclosure of information pertaining to an SIO, by its very nature, carries a greater risk of harm, both in jeopardising the safety of participants and in potentially limiting the Organisation’s intelligence-gathering capability by compromising the integrity of the operation.

586. Subsection (4) provides that section 15.4 of the Criminal Code (extended geographical jurisdiction—category D) applies to the offences in section 35P. This means that the offences apply to any person, in respect of conduct engaged in any country, whether or not the conduct is an offence under the laws of the relevant local jurisdiction (if outside Australia). This form of extended geographical jurisdiction is necessary to ensure that the offences apply to SIO participants or persons who have knowledge of an SIO who are not Australian citizens and who engage in unauthorised disclosures outside Australia. Given the potential of information obtained under an SIO to place at risk Australia’s national security and intelligence gathering capabilities, in addition to potentially endangering SIO participants, it is appropriate that the offences have the widest possible geographical application to target such wrongdoing. Prosecutions of non-Australians in relation to conduct outside Australia is subject to the safeguard in section 16.1 of the Criminal Code, which requires the Attorney-General to consent to the commencement of such prosecutions.

587. Subsection 35P(5) provides that subsection 35P(4) does not, by implication, affect the interpretation of any other provision in the ASIO Act. This provision is necessary because some offences in the ASIO Act were enacted prior to the commencement of the extended geographical jurisdiction provisions of Part 2.7 of the Criminal Code on 24 May 2001. As such, the geographical jurisdiction of any pre-2001 offence provisions which do not provide for the application of Part 2.7 of the Criminal Code is assessed in accordance with ordinary principles of statutory interpretation. Subsection 35P(5) makes clear that the inclusion of subsection 35P(4) in relation to new section 35P is not intended to have any impact on the interpretation of the geographical jurisdiction applying to any offence provision in the ASIO Act enacted prior to 24 May 2001.
The Explanatory Memorandum to the NSLAB (No 1) 2014 also includes a ‘Statement of compatibility with human rights’ prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011. The relevant part is as follows:

**New offences**

76. The Schedule will create two new offences in new section 35P relating to the unauthorised disclosure of information relating to an SIO, one being an aggravated offence, with penalties of five and ten years imprisonment. These offences are necessary to protect persons participating in an SIO and will ensure the integrity of operations, by creating a deterrent to unauthorised disclosures, which may place at risk the safety of participants or the effective conduct of the operation. The relevant aggravating elements are an intention of endangering the health or safety of any person, or prejudicing the effective conduct of an SIO or that the disclosure will endanger the health or safety of any person or prejudice the effective conduct of an SIO. The offences apply to disclosures by any person, including for example, participants in an SIO, other persons to whom information about an SIO has been communicated in an official capacity and persons who are the recipients of an unauthorised disclosure of information. The offences have statutory defences—including disclosures pertaining to the operation of Division 4 or legal proceedings relating to Division 4, other legal obligations of disclosure and the performance by ASIO of its statutory functions.

77. The fault element of intention applies to the physical element of a person’s conduct in relation to both offences, by reason of subsection 5.6(1) of the Criminal Code. The fault element of recklessness applies to the physical element of the circumstance that the information relates to an SIO, by reason of subsection 5.6(2) of the Criminal Code. This means that the person must have been aware of a substantial risk that the information related to a special intelligence operation, but nonetheless and unjustifiably in the circumstances took the risk of making the disclosure. Accordingly, a person who is wholly unaware of the existence of a special intelligence operation, and discloses information, is unlikely to meet the threshold of recklessness.

**Freedom of expression—Article 19(2) of the ICCPR**

78. Article 19(2) of the ICCPR provides that everyone has the right to freedom of expression, including the freedom to receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art or through any other media. Article 19(3) provides
that this right may be limited if it is necessary to achieve a legitimate purpose, including national security. Any limitation must be established by law and be reasonable and proportionate to achieve a legitimate objective.

79. These offences engage and limit the right to freedom of expression in that they prohibit the disclosure of information relating to an SIO, including publication of such information. The limitation is to achieve a permissible purpose set out in Article 19(3), being matters of national security. These offences are necessary to achieve the legitimate objective of protecting persons participating in an SIO and to ensure the integrity of operations related to national security, by creating a deterrent to unauthorised disclosures, which may place at risk the safety of participants or the effective conduct of the operation. The offences apply to disclosures by any person, including participants in an SIO, other persons to whom information about an SIO has been communicated in an official capacity and persons who are the recipients of an unauthorised disclosure of information, should they engage in any subsequent disclosure for these reasons.

80. Communicating such sensitive information can place the health and safety of participants at risk, negates the integrity of operations in general and affects the conduct of the operation in question. As such, the limitation on the right is necessary for the protection of national security and the health and safety of participants. It is reasonable as the offence provides appropriate defences and retains important safeguards facilitating the operation of oversight and accountability bodies. For example, the offence would not apply through subsection 18(9) of the IGIS Act if a document was dealt with for the purpose of producing information under subsection 18(1) of the IGIS Act. Further, the offence would not apply in accordance with section 10 of the Public Interest Disclosure Act 2013 (PID Act) if information was dealt with for the purpose of making a public interest disclosure in accordance with the PID Act as it applies to ASIO. For example, a person could report a matter in relation to an SIO to internal authorised officers or the IGIS. To avoid any doubt, the offences further contain express exceptions for disclosures to the IGIS or his or her staff, and the IGIS and his or her staff in connection with their statutory oversight duties.

81. These limitations on Article 19(2) are for a permissible purpose as set out in Article 19(3), are necessary to achieve a legitimate objective which is protecting persons participating in an SIO and to ensure the integrity of
operations, are provided for by law and are reasonable and proportionate to achieve this objective.

**Scrutiny of the NSLAB (No 1) 2014 by the Parliamentary Joint Committee on Human Rights**

The functions of the Parliamentary Joint Committee on Human Rights under the *Human Rights (Parliamentary Scrutiny) Act 2011* include to examine Bills for Acts that come before either House of the Parliament for compatibility with human rights and to examine Acts for compatibility with human rights.

In its *Sixteenth Report of the 44th Parliament* (25 November 2014), that Committee concluded as follows in relation to the offences—after the NSLAB (No 1) 2014 had become law, and in light of the Minister’s response that the Government did not intend to supplement the material provided in the Statement in the Explanatory Memorandum:

2.107 The committee considers that the offence provisions have not been shown to be a reasonable, necessary and proportionate limitation. On this question, the statement of compatibility relies on the existence of defences and safeguards as facilitating the operation of oversight and accountability bodies in respect of the measure.

2.108 However, the committee notes that, as the non-aggravated offence applies to conduct which is done recklessly rather than intentionally, a journalist could be found guilty of an offence even though they did not intentionally disclose information about a SIO. As SIOs can cover virtually all of ASIO’s activities, the committee considers that these offences could discourage journalists from legitimate reporting of ASIO’s activities for fear of falling foul of this offence provision. This concern is compounded by the fact that, without a direct confirmation from ASIO, it would be difficult for a journalist to accurately determine whether conduct by ASIO is pursuant to a SIO or other intelligence gathering power.

2.109 The committee notes that the potential ‘chilling effect’ of the new offences on journalists reporting on ASIO activities raises [sic] could undermine public reporting and scrutiny of ASIO’s activities, such as in cases where it is alleged that mistakes have been made by ASIO.

2.110 The committee notes that the available defences are primarily designed to protect disclosure to the IGIS. The committee notes that there is no general defence related to public reporting in the public interest or general protections for whistleblowers other than for disclosure to the IGIS. The defence provisions can therefore reasonably be described as
very narrow, and the committee considers that they do not offer adequate protection of the public interest in respect of public reporting.

2.111 The committee therefore considers that, in light of these considerations, the Attorney-General has not demonstrated that the offence provisions are reasonable or proportionate limitations on the right to freedom of expression.

2.112 On the information provided, the committee considers that the new offence provisions for disclosing information regarding SIOs are incompatible with the right to freedom of expression because the provisions appear to impose disproportionate limits on that right.

The Government response to the Committee’s conclusion, as reflected in an AGD/ASIO submission to this inquiry, was as follows:

The Attorney-General has also written to that Committee, indicating that the Government is satisfied that all measures in the National Security Legislation Amendment Act (No 1) 2014 are compliant with Australia’s human rights obligations following careful consideration in the development of the legislation, and expressing concern that the Committee’s methodology in reaching conclusions about the compatibility or otherwise of measures appears to be informed by considerations of form rather than substance.

Section 35P comes into operation

Section 35P came into operation on 30 October 2014. Section 35P provides as follows, with changes from the NSLAB (No 1) 2014 highlighted in yellow:

35P Unauthorised disclosure of information

Unauthorised disclosure of information

(1) A person commits an offence if:
(a) the person discloses information; and
(b) the information relates to a special intelligence operation.

Penalty: Imprisonment for 5 years.

Note: Recklessness is the fault element for the circumstances described in paragraph (1)(b)—see section 5.6 of the Criminal Code.

Unauthorised disclosure of information—endangering safety, etc.

(2) A person commits an offence if:
(a) the person discloses information; and
(b) the information relates to a special intelligence operation; and
(c) either:

(i) the person intends to endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation; or

(ii) the disclosure of the information will endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation.

Penalty: Imprisonment for 10 years.

Note: Recklessness is the fault element for the circumstances described in paragraph (2)(b)—see section 5.6 of the Criminal Code.

Exceptions

(3) Subsections (1) and (2) do not apply if the disclosure was:

(a) in connection with the administration or execution of this Division; or

(b) for the purposes of any legal proceedings arising out of or otherwise related to this Division or of any report of any such proceedings; or

(c) in accordance with any requirement imposed by law; or

(d) in connection with the performance of functions or duties, or the exercise of powers, of the Organisation; or

(e) for the purpose of obtaining legal advice in relation to the special intelligence operation; or

(f) to an IGIS official for the purpose of the Inspector-General of Intelligence and Security exercising powers, or performing functions or duties, under the Inspector-General of Intelligence and Security Act 1986; or

(g) by an IGIS official in connection with the IGIS official exercising powers, or performing functions or duties, under that Act.

Note: A defendant bears an evidential burden in relation to the matters in this subsection—see subsection 13.3(3) of the Criminal Code.

Extended geographical jurisdiction

(4) Section 15.4 of the Criminal Code (extended geographical jurisdiction—category D) applies to an offence against subsection (1) or (2).

(5) Subsection (4) does not, by implication, affect the interpretation of any other provision of this Act.
Appendix C—Post-enactment safeguards

The *Prosecution Policy of the Commonwealth* prepared by the Commonwealth Director of Public Prosecutions (CDPP) requires the CDPP to take into consideration the public interest in commencing or continuing a prosecution (paragraphs [2.8]–[2.10]).

Further:

- on 29 October 2014 the CDPP issued a National Legal Direction, *Prosecuting offences for unauthorised disclosure of information relating to controlled operations, special intelligence operations or delayed notification search warrants*, requiring prosecutors to seek the personal approval of the CDPP to any proposed prosecutions of offences against section 35P, and
- on 30 October 2014 the Attorney-General issued a direction to the CDPP under section 8 of the Director of Public Prosecutions Act 1983 requiring the CDPP to obtain the consent of the Attorney-General to the prosecution of a journalist for certain offences including offences against section 35P where the facts constituting the alleged offence relate to the work of the person in a professional capacity as a journalist.

The first of these directions was updated on updated to 1 December 2014. These directions read as follows (omitting footnotes):

**CDPP National Legal Directions**

**Controlled operations**

1. Part IAB of the *Crimes Act 1914* (*Crimes Act*) establishes a statutory framework for the authorisation, conduct and monitoring of ‘controlled operations’. These are police operations which involve the participation of law enforcement officers and which are carried out for the purpose of obtaining evidence that may lead to the prosecution of a person for a serious Commonwealth offence or a serious State offence that has a federal aspect. The controlled operations framework established under the *Crimes Act* has been operating since 1996.

2. A controlled operations authority may authorise a law enforcement officer, or other person, to engage in conduct which would, but for these provisions, constitute a Commonwealth offence or an offence against a law of a State or Territory. Such an authority enables law enforcement to work undercover to infiltrate criminal syndicates, gain the confidence of criminals and gather valuable evidence of serious criminal conduct. The authority protects the undercover operative from any potential criminal liability and ensures that any evidence is lawfully collected and can be used in subsequent criminal prosecutions. This can be very dangerous work. Should the true identity of an
undercover operative be revealed, he or she may be at serious risk of serious harm. To protect the integrity of controlled operations, s.15HK and s.15HL of the Crimes Act make it a criminal offence to disclose information relating to a controlled operation. These disclosure offences were inserted into the Crimes Act in 2010.

**Special intelligence operations**

3. On 30 October 2014 the *Australian Security Intelligence Organisation Act 1979 (ASIO Act)* was amended to establish a similar statutory framework for the conduct of ‘special intelligence operations’ by ASIO. These are intelligence operations carried out for a purpose relevant to key ASIO statutory functions. Whilst the special intelligence operations framework is based broadly on the controlled operations framework in the Crimes Act, appropriate modifications have been made to reflect the difference between a law enforcement operation, which is conducted in order to investigate a serious offence and gather admissible evidence, and a covert intelligence gathering operation, which is conducted for national security purposes. This framework, which is contained in Division 4 of the ASIO Act, commenced operation on 30 October 2014.

4. Like a controlled operation authority, a special intelligence operation authority may authorise a person to engage in conduct which would, but for these provisions, be subject to civil or criminal liability under a law of the Commonwealth, a State or Territory. Such an authority will enable a person to work undercover to collect sensitive information by covert means. The authority will protect such a person from any potential civil or criminal liability. Like undercover police work, special intelligence operations may expose those involved to serious risk of serious harm should the true identity of such a person be revealed. To protect the integrity of special intelligence operations, s.35P(1) and s.35P(2) of the ASIO Act make it a criminal offence to disclose information relating to a special intelligence operation.

5. The statutory framework for special intelligence operations was inserted into the ASIO Act by the *National Security Legislation Amendment Act (No.1) 2014*. An *Advisory Report on the National Security Legislation Amendment Bill (No.1) 2014*, prepared by the Parliamentary Joint Committee on Intelligence and Security in September 2014, recommended that the Bill or Explanatory Memorandum of the Bill be clarified to confirm that the Commonwealth Director of Public Prosecutions (CDPP) would take into account the public interest, including the public interest in publication, before initiating a prosecution for an offence of disclosing a special intelligence operation.
6. Following consideration of the Advisory Report by Government, a Revised Explanatory Memorandum to the National Security Legislation Amendment Bill (No.1) 2014 was issued. Paragraph 582 of the Revised Explanatory Memorandum states as follows:

‘Subsection 35P(3) does not include an express defence for the communication of information relating to a special intelligence operation, where such communication is found to be in the public interest. The Commonwealth Director of Public Prosecutions (CDPP) is required, under the Prosecution Policy of the Commonwealth, to consider the public interest in the commencement or continuation of a prosecution. It would be open to the CDPP, in making independent decisions on this matter, to have regard to any public interest in the communication of information in particular instances as the CDPP considers appropriate.’

Delayed Notification Search Warrants

7. On 1 December 2014 Part IAAA was inserted into the Crimes Act to establish a delayed notification search warrant scheme for eligible federal offences. Prior to the introduction of this scheme, an officer executing a Crimes Act search warrant at a premises was required to identify himself or herself to the occupier of the premises and make available to that person a copy of the search warrant. There was no scope for federal law enforcement officers to search premises covertly without them immediately notifying the occupier. Under the delayed notification search warrant scheme, a member of the Australian Federal Police can apply for a search warrant which specifically authorises police to conduct a search of premises without the occupier’s knowledge and without notifying the occupier of the premises at the time the warrant is executed. This scheme commenced operation on 1 December 2014.

8. Whilst notice of the search is ultimately required to be given to the occupier of the searched premises, that notice may be delayed but should generally be given within 6 months. Delayed notification search warrants enable federal law enforcement authorities to maintain the integrity of covert police investigations for terrorism offences. If members of a terrorist group are alerted to investigator’s knowledge of their activities, the success of any law enforcement operation could be jeopardised. To protect the integrity of these law enforcement operations, s.3ZZHA of the Crimes Act makes it a criminal offence to disclose information relating to a delayed notification search warrant prior to such notice being provided to the occupier of the premises.

9. The statutory framework for the delayed notification search warrant scheme was inserted into the Crimes Act by the Counter-Terrorism legislation
Amendment (Foreign Fighters) Act 2014. An Advisory Report on the Counter-Terrorism legislation Amendment (Foreign Fighters) Act 2014, prepared by the Parliamentary Joint Committee on Intelligence and Security in October 2014, recommended that the Explanatory Memorandum of the Bill be amended to confirm that the CDPP must take into account the public interest, including the public interest in publication, before initiating a prosecution for an offence of disclosing information relating to a delayed notification search warrant.

10. Following consideration of the Advisory Report by Government, a Revised Explanatory Memorandum to the Counter-Terrorism legislation Amendment (Foreign Fighters) Act 2014 was issued. Paragraph 689 of the Revised Explanatory Memorandum states as follows:

‘Under the Prosecution Policy of the Commonwealth, the Commonwealth Director of Public Prosecutions (CDPP) is required to consider the public interest in the commencement or continuation of a prosecution. It would be open to the CDPP, in making independent decisions on this matter, to have regard to any public interest in the disclosure of information in particular instances as the CDPP considers appropriate.’

Offences to which this National Legal Direction applies

11. This National Legal Direction applies to any matter involving the prosecution or possible prosecution of the following offences (hereafter referred to as ‘relevant unauthorised disclosure offences’) which are set out in full in the enclosed Schedule One:

- Unauthorised disclosure of information relating to a controlled operation contrary to s.15HK of the Crimes Act.
- Unauthorised disclosure of information relating to a controlled operation where the disclosure is intended or will endanger the health or safety of any person or prejudice the effective conduct of a controlled operation contrary to s.15HL of the Crimes Act.
- Unauthorised disclosure of information relating to a special intelligence operation contrary to s.35P(1) of the ASIO Act.
- Unauthorised disclosure of information relating to a special intelligence operation where the disclosure is intended or will endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation contrary to s.35P(2) of the ASIO Act.
- Unauthorised disclosure of information relating to a delayed notification search warrant contrary to s.3ZZHA of the Crimes Act.
Public Interest Considerations

12. Decisions about the commencement and continuation of prosecutions are made by the CDPP independent of Government in accordance with the Prosecution Policy of the Commonwealth. Under the Prosecution Policy of the Commonwealth, a prosecutor who has satisfied himself or herself that the evidence is sufficient to justify the institution or continuation of a prosecution must then consider whether the public interest requires a prosecution to be pursued. Not all offences brought to the attention of the authorities must be prosecuted.

13. The factors which can properly be taken into account in deciding whether the public interest requires a prosecution will vary from case to case. Paragraph 2.10 of the Prosecution Policy of the Commonwealth sets out a list of factors which may arise for consideration in determining whether the public interest requires a prosecution to take place.

14. In making a decision about the commencement or continuation of a prosecution for a relevant unauthorised disclosure offence, a prosecutor must apply the Prosecution Policy of the Commonwealth. In accordance with that policy, a prosecutor must consider whether the public interest requires a prosecution to be pursued.

15. In addition to any other relevant factors which should properly be taken into account in determining whether the public interest requires a prosecution, a prosecutor must take into account whether the disclosure of the relevant information, including the manner, form and timing of such disclosure, was in the public interest (as opposed to being merely of public interest). The timing of such disclosure, will be particularly relevant in the case of delayed notification search warrants given that notice of the search is ultimately required to be given to the occupier and that no offence is committed where disclosure is made after such notice has been given.

16. While each case must be considered on its merits, where a prosecutor concludes that the ‘disclosure of the relevant information was in the public interest, it will be more difficult to conclude that a prosecution for a relevant unauthorised disclosure offence is justified. If the question is finely balanced, the CDPP may provide a prospective defendant an opportunity to make submissions as to why a particular disclosure was in the public interest, such that a prosecution should not take place.

Consent of the Attorney-General

17. On 30 October 2014 the Attorney-General (‘the Attorney’) issued a Ministerial Direction to the Director of Public Prosecutions (‘the Director’) pursuant to
s.8(1) of the *Director of Public Prosecutions Act 1983*. The Attorney directed the Director not proceed with a prosecution of a person for alleged contravention of a relevant unauthorised disclosure offence without the written consent of the Attorney where the person is a journalist and the facts constituting the alleged offence relate to the work of the person in a professional capacity as a journalist. A copy of this Ministerial Direction is set out in the enclosed Schedule Two.

18. The consent of the Attorney will only be sought in matters that meet the threshold required by the *Prosecution Policy of the Commonwealth*. The consent of the Attorney will not be sought in matters where there is insufficient evidence to justify the institution or continuation of a prosecution or where a prosecution would not be in the public interest.

**Consent of the Director**

19. Subject to the requirements imposed by the Ministerial Direction referred to above, all decisions regarding the commencement or continuation of a prosecution for a relevant unauthorised disclosure offence must be made personally by the Director.

Robert Bromwich  
Director of Public Prosecutions  
Date: 1 December 2014
Ministerial Direction (Commonwealth Director of Public Prosecutions)

Director of Public Prosecutions Act 1983

I George Brandis QC, Attorney-General of Australia, having consulted the Director of Public Prosecutions (‘the Director’), give the following direction under subsection 8(1) of the Director of Public prosecutions Act 1983.

The Director must not proceed with a prosecution of a person for alleged contravention of the following sections without the written consent of the Attorney-General:

(a) section 35P of the Australian Security Intelligence Organisation Act 1979
(b) section 15HK of the Crimes Act 1914
(c) section 15HL of the Crimes Act 1914
(d) section 3ZZHA of the Crimes Act 1914

where the person is a journalist and the facts constituting the alleged offence relate to the work of the person in a professional capacity as a journalist.

Dated 30 October 2014

[signed]

The Hon George Brandis QC
Attorney-General
Appendix D—A selection of criticisms and comments about section 35P from submissions to the inquiry

Broad legal and policy matters

- Australia does not have constitutional or legislative protections of free speech and human rights comparable to those of other similar countries.

- The oversight of Australia’s intelligence agencies is poor, including by international standards:
  - While the oversight of Australia’s intelligence agencies by the IGIS is important, it is not sufficient.

- Legislation which authorises ASIO officers to commit crimes and prevents reporting of those crimes is greatly troubling.

- Section 35P is unnecessary because existing Commonwealth secrecy offences are adequate.

- The basic offence in section 35P(1) should contain an express requirement of harm to the public interest.

- It is difficult to know whether information ‘relates to’ an SIO when an SIO could relate to a broad range of ASIO activities:
  - Information need only ‘relate to’ an SIO in a minor or indirect way.
  - The capacity to declare an SIO could be open to abuse by the Government.

- The section 35P offences are far too broad:
  - As such, section 35P is beyond the scope of the defence power and inconsistent with the constitutional implied freedom of political communication.
  - Section 35P is inconsistent with international human rights law including Article 19 of the International Covenant on Civil and Political Rights (ICCPR).

- Illegality (including acts not even able to be authorised as part of an SIO) and other substantial wrongdoing ought to be able to be discussed openly.

- There is no protection under the Public Interest Disclosure Act 2013 for intelligence agency officers making disclosures to journalists even if these are manifestly in the public interest.
• The basic offence may apply (including to journalists) even if no harm eventuates and the disclosure was not intended to cause harm.

• To ‘prejudice the effective conduct’ of an SIO may involve the most minor of inconveniences or administrative burdens.

• The section 35P offences have no time limits—the risk of prosecution continues in perpetuity.

• Section 35P will inhibit discussion relating to ASIO activities generally and for all time, including by journalists and academics.

• There is inadequate provision for exceptions, including in relation to information which has already been reported in the international media:
  – There should be a public interest exception and a defence for information already in the public domain.

Comments by or concerning journalists

• The media should have been much more agitated about the introduction of the controlled operations offences in 2010:
  – The media is now aware of outright restrictions on and increasing difficulties associated with public interest reporting.
  – Further, the veil of secrecy does not exist in the same way in the controlled operations context as it does regarding intelligence gathering and intelligence operations.

• Journalists may unwittingly commit offences and be convicted and jailed.

• Fear of prosecution may chill discussion by journalists of matters (including actual or suspected illegal activity) relating to government.

• Section 35P will discourage whistleblowers from approaching the media, journalists from pursuing stories and editors from publishing stories.

• Section 35P will prevent not only publication of information which ‘relates to’ an SIO but of discussions between journalists and sources and between journalists and editors which concern such information.
A journalist might be unlikely to contact the authorities in the early stages of an investigation because:

- the authorities might shut down the story on the basis that it ‘relates to’ an SIO, even if the link is only tenuous, and
- that action could prompt surveillance of the journalist or a source.

There is no permitted way by which a journalist can publish information which relates to an SIO.

It is not the duty of the media or the public to keep ASIO operations secret—that duty belongs to ASIO, its partner agencies and officials and MPs to whom it discloses operations.

- It is the duty of the media to reveal any excesses, or potential excesses, by ASIO and its partners.

Section 35P could lead to a situation in which the ordinary activities of ASIO are placed beyond the realms of a journalist’s capacity to report.

Section 35P will trigger the power for ASIO and law enforcement agencies to access journalists’ telecommunications data to identify confidential sources.

A study conducted in the United States shows that journalists’ practices have changed (adopting some aspects of ‘spy’ tradecraft) in response to the empowering of national security agencies.

- Many journalists believed that the United States Government had collected their communications data.

Section 35P will deter constructive consultation between security and intelligence agencies and the media.

- Whistleblowers will still make disclosures and ‘become martyrs’ and the chances are they may bypass the established media and separately disclose information which has not been responsibly filtered.

The directions given by the CDPP and the Attorney-General in October 2014 in relation to whether a prosecution will be initiated in a particular case is not an effective safeguard or comfort to journalists.
Appendix E—A selection of proposals for reform from submissions to the inquiry

Thematic suggestions

- Section 35P as a whole should be repealed (this was suggested in several submissions).
- The basic offence in section 35P(1) should be repealed (this was suggested in quite a large number of submissions).
- A public interest defence to the offences should be provided (this was suggested in quite a large number of submissions).
  - This could be limited to circumstances where illegality, substantial misconduct or other forms of impropriety are involved.
- There should be a defence available in relation to disclosure of information which is already in the public domain.
- Disclosures to Federal and State Members of Parliament should be protected when a citizen has concerns about the legality or appropriateness of a security operation.
- The exception in relation to legal advice should extend to legal advice about the subject of the offence (the disclosure or proposed disclosure).
- The basic offence in section 35P(1) should be amended to include an express requirement of harm, like section 35P(2).
- The offences should be defined with more precision—the words ‘relates to’ are too broad.
- The offences should have a specified duration.
- Section 35P(2) should be reviewed and restructured.
- The offences should be limited to circumstances where a person intends to harm the public interest:
  - Alternatively, the penalties should be adjusted to reflect the fact that unintended harm is less serious.
- The fault element of knowledge should replace the fault element of recklessness (as to the physical element involving that the information relates to an SIO).
• Journalists should be exempted from the offences:
  – In this context, defining ‘journalist’ might be problematical and such differential treatment might be objectionable in principle.
• Existing and any future safeguards of freedom of expression applicable in relation to journalists should also be extended to the academic profession acting in that capacity.

Specific proposed suggestions (proposed draft provisions)

Seven West Media

A new paragraph of section 35P(3) would provide that the offences do not apply if the disclosure was:

• made in good faith in a report or commentary published about a matter of public interest by a person engaged in a professional capacity as a journalist, where the report or commentary does not disclose, directly or by inference, the identity of a security officer.

This would be followed by a new subsection along the following lines:

• Without limiting the generality of [the new paragraph], a disclosure is about a matter of public interest for the purposes of [the new paragraph] if it is or relates to:
  – a matter that increases the ability of the public to scrutinise issues of national security, including security activities or Government policy
  – a matter that contributes to the public debate on national security matters or related issues
  – conduct that, but for the provisions of this Act:
    ▪ contravenes a law of the Commonwealth, a State or a Territory
    ▪ contravenes a law of a foreign country
    ▪ perverts, or is engaged in for the purpose of perverting, or attempting to pervert, the course of justice
    ▪ involves, or is engaged in for the purpose of, corruption of any other kind
    ▪ constitutes maladministration
    ▪ is an abuse of public trust
- involves, or is engaged in for the purpose of, a public official abusing his or her position as a public official
- could, if proved, give reasonable grounds for disciplinary action against a public official.

**Senator Xenophon and Dr Fernandes**

A public interest exemption was proposed as an amendment in the Senate as part of the debate relating to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 (See *Hansard*, Senate, 26 March 2015 at 102).

This suggestion was as an alternative, that is, if section 35P were not to be repealed:

- The basic offence would be the same but have an additional element, namely that the person *knows* that the information relates to an SIO.
- The aggravated offence would be the same as the proposed basic offence but with an express harm requirement, namely that the person *intends* the disclosure of information to endanger the health or safety of any person or prejudice the effective conduct of an SIO.

A new paragraph of section 35P(3) would provide that the offences do not apply if the disclosure was:

- by a person who was working in a professional capacity as a journalist, or an employer of such a person
- published in good faith in a report or commentary about a matter of public interest, and
- the report was not likely to enable an ASIO employee, ASIO affiliate, a staff member of ASIS or an IGIS official to be identified.

This would be followed by a new subsection along the following lines:

- Without limiting the generality of [the new paragraph], a disclosure is about a matter of public interest if it relates to one or more of the following:
  - conduct that:
    - contravenes a law of the Commonwealth, a State or Territory
    - contravenes a law of a foreign country
    - is engaged in for the purpose of perverting, or attempting to pervert, the course of justice
is engaged in for the purpose of corruption
constitutes maladministration
constitutes an abuse of public trust
involves an official of a public agency abusing his or her position as an official of that agency, or
could, if proved, give reasonable grounds for disciplinary action against an official of a public agency.

**Australian Lawyers for Human Rights**

The suggestion is that a section along the following lines be added to the Act.

- No person is guilty of an offence under section 35P if the person establishes that he or she acted in the public interest.

- Subject to the following provision [in deciding], a person acts in the public interest if:
  - the person acts for the purpose of disclosing an offence under an Act of Parliament, or similar substantial or serious misfeasance, whether or not amounting to an offence, that he or she reasonably believes has been, is being or is about to be committed by another person in the purported performance of that person’s functions for or on behalf of the Government of Australia, and/or
  - the public interest in the disclosure on balance outweighs the public interest in non-disclosure.

- In deciding whether the public interest in the disclosure on balance outweighs the public interest in non-disclosure, a judge or court must consider:
  - the seriousness of the alleged offence
  - whether the person had reasonable grounds to believe that the disclosure would be in the public interest
  - the nature of the public interest intended to be served by the disclosure
  - the person’s reasonable belief as to the extent of the harm or risk of harm created by the disclosure
  - the person’s reasonable belief as to the extent of the harm or risk of harm created by non-disclosure of the information
whether the person tried other reasonably accessible alternatives before making the disclosure in the way that they made it

whether no more information was publicly disclosed than the person believed was reasonably necessary in the light of their perception of the extent or risk of harm involved, and

the existence of exigent circumstances justifying the disclosure (including, but not limited to, whether the communication of the information was necessary to avoid grievous bodily harm or death).

Councills for civil liberties across Australia

The suggestion is that the offences would not apply if the disclosure was made by either:

- a journalist in the ordinary course of their work, or
- an informant who gives information to a journalist in the expectation that the information may be published in a news medium, and

either

- the journalist did not intend to endanger the health or safety of any person or prejudice the effective conduct of an SIO, or
- the disclosure exposes conduct by ASIO, a government department or agency, or any other entity or person involved in an SIO that may be capable of constituting:
  - conduct involved in the SIO that:
    - involves the death of, or serious injury to, any person
    - constitutes torture
    - involves the commission of a sexual offence against any person, or
    - results in significant loss of, or serious damage to, property, or
  - misconduct by ASIO, a government department or agency, or any other entity or person involved in an SIO, or
  - a power exercised for an improper purpose by ASIO, a government department or agency, or any other entity or person involved in an SIO that is beyond the scope of an SIO authority, or
- the disclosure was otherwise in the public interest.
• A defendant who wishes to deny criminal responsibility by relying on the second of the preceding three points [disclosure exposes conduct] would bear an evidential burden in relation to that matter.

**Joint Media Organisations**

The suggestions is that sections 35P(1) and (2) remain the same but with *knowledge* rather than recklessness as the fault element attaching to the circumstance that the information relates to an SIO.

A new paragraph of section 35P(3) would provide that the offences do not apply if the disclosure was:

• made in good faith for the purpose of the information being published in a report or commentary about a matter in the public interest.

(An alternative form of words for the additional exception could be for a disclosure made in good faith in a report or commentary published about a matter of public interest by a person engaged in a professional capacity as a journalist where the report or commentary does not disclose, directly or by inference, the identity of a security officer.)

This would be followed by a new subsection along the following lines:

• Without limiting the generality of [the new paragraph], a disclosure is about a matter of public interest for the purposes of [the new paragraph] if it is or relates to:
  – a matter that increases the ability of the public to scrutinise issues of national security, including security activities or Government policy, or
  – a matter that contributes to the public debate on national security matters or related issues
  – conduct that, but for the provisions of this Act:
    ▪ contravenes a law of the Commonwealth, a State or a Territory
    ▪ contravenes a law of a foreign country
    ▪ perverts, or is engaged in for the purpose of perverting, or attempting to pervert, the course of justice
    ▪ involves, or is engaged in for the purpose of, corruption of any other kind
    ▪ constitutes maladministration
    ▪ is an abuse of public trust
• involves, or is engaged in for the purpose of, a public official abusing his or her position as a public official

• could, if provided, give reasonable grounds for disciplinary action against a public official.
Appendix F—AGD and ASIO response to certain criticisms

The joint submission from the Attorney-General’s Department (AGD) and ASIO (Submission 8 to this inquiry) included the following summary of media and stakeholder concerns expressed about section 35P and a response to certain proposed amendments to section 35P (footnotes omitted):

**Media and stakeholder commentary—section 35P**

The proposed inclusion of section 35P in the SIO scheme was the subject of considerable media and stakeholder commentary on the Bill, including in evidence to the PJCIS inquiry into the Bill. The key concern raised was that the offences are overly broad and could suppress or limit legitimate reporting of national security matters, particularly instances of wrongdoing or suspected wrongdoing. Specific criticisms and concerns include:

- the offences may have a chilling effect on journalism because they may criminalise (or be perceived as criminalising) reporting on suspected instances of wrongdoing in the course of SIOs, notwithstanding that there is a legitimate public interest in the disclosure of such wrongdoing. (For example, the causation of death in the course of an operation, or activities that otherwise grossly exceed the limits of an SIO authority);

- the potential for the SIO scheme to be abused by the declaration of operations for illegitimate purposes, such as to prevent the public disclosure of information about certain activities to avoid embarrassment or inconvenience rather than to protect security;

- the potential for journalists and other disclosers to unwittingly commit the basic offence by disclosing information about ASIO’s activities, which they did not know were undertaken as part of an SIO;

- the potential for the basic offence to apply to journalists or others, notwithstanding that no harm in fact eventuates from the disclosure, and that the disclosure was not intended to cause harm; and

- the fact that the offences are not time limited, such that the disclosure of information relating to operations conducted and concluded years or decades ago could be the subject of a prosecution, notwithstanding there is no harm sustained due to the passage of time.
A number of amendments were proposed by various stakeholders, including:

- repealing the offences, and relying on disclosure offences of general application, such as those in section 92 of the ASIO Act (publication of the identity of ASIO personnel) or in the general offences in Part VII of the Crimes Act (official secrets);
- repealing the basic offence in subsection 35P(1), leaving only the aggravated offence in subsection 35P(2), which requires proof of intention to cause harm in making the disclosure, or proof that the disclosure will cause harm (with some further proposals that the maximum penalty for the aggravated offence should be reduced);
- replacing the fault element of recklessness as to the circumstance that information related to an SIO with that of knowledge (in both the basic and aggravated offences);
- the insertion of an offence-specific defence for disclosures made in the public interest;
- the insertion of an offence-specific defence for journalists who report on national security operations in the public interest;
- the insertion of an offence-specific defence for information already in the public domain;
- the insertion of a statutory sentencing criteria, including requirements that sentencing courts must specifically consider the public interest, if any, in the disclosure of information constituting the offence;
- the insertion of a sunset provision applying to the SIO scheme as a whole, including section 35P, with a requirement that the PJCIS or the INSLM review the scheme prior to its expiry; and
- deferring the establishment of the SIO scheme and referring it to an INSLM (once appointed) for an opinion on whether it should be pursued, including specific consideration of whether the proposed disclosure offences in section 35P are necessary and appropriate.

Comments on stakeholders’ proposed amendments to section 35P

As mentioned above, AGD and ASIO gave extensive evidence to Parliamentary committees considering the (then) Bill about the Government’s position on a number of proposed amendments to section 35P. The Attorney-General also provided responses to relevant matters arising in the course of the debate of the Bill in the Senate. The legal and legal policy issues arising in relation to the key suggested
amendments are summarised below. More extensive analysis is contained in the Department’s and ASIO’s submissions to the PJCIS and the Senate Scrutiny of Bills Committee inquiries into the Bill.

...  

Exceptions—public interest disclosures or journalistic reporting

Stakeholder suggestion

As mentioned above, several stakeholders have argued in favour of additional exceptions to the offences. Key proposals include either a specific exception to the offences in favour of journalists, or a general public interest exception, where the trier of fact is of the view that the public interest in making a disclosure outweighed the detriment to security.

Comments

The offences in section 35P intentionally apply to all persons, irrespective of their position, profession or motivation, consistent with the intention to avoid the significant risks arising from the very fact of disclosure of information about an SIO. The Government has indicated it has strong reservations about either of these proposed exceptions for several reasons, which were addressed in detail in the submissions of the Department and ASIO to the PJCIS inquiry into the Bill (as enclosed in the accompanying volume of materials).

In short, these reasons are, first, that it is contrary to the criminal law policy of the Commonwealth to create specific exceptions in favour of classes of persons (such as journalists) from the legal obligations of non-disclosure to which all other Australian persons and bodies are subject. It is appropriate that all members of the community are expected to adhere to non-disclosure obligations, which should apply equally to all persons – whether they are intelligence or law enforcement professionals or journalists reporting on national security matters. The absence of exceptions in favour of specific classes of persons is also consistent with the policy intention that the offences are directed to the risks posed to security as a result of the disclosure of sensitive information, which arise irrespective of the motives or identity of the discloser.

Secondly, a general public interest defence is not considered necessary or appropriate for two reasons. There is already an exception in subsection 35P(3) for internal disclosures of suspected wrongdoing in relation to an SIO to the IGIS. Public officials can also avail themselves of the internal disclosure provisions of the Public Interest Disclosure Act 2013, which overrides secrecy laws of general application. The IGIS Act further overrides secrecy laws of general application in relation to persons who comply with notices for the production of documents or the provision of information issued under that Act.
In addition, a dedicated public interest defence is not considered appropriate in relation to the offences in proposed subsections 35P(1) and 35P(2). This is because, even if a jury or a trial judge as the final arbiter of fact held that a disclosure was not in the public interest, the disclosure would have already occurred and the potential for harm actualised. Prejudice to security, and consequently harm to the public interest from a disclosure relating to an SIO, can evolve quickly, such as reprisals from persons being investigated. Harm could also evolve so slowly as to be difficult to detect—for example, the disclosure of a person’s identity as an ASIO employee or an ASIO affiliate could be used by foreign intelligence services to target and infiltrate ASIO and its operations, or compromise its staff, over a significant period of time.

Further, a public interest defence would inappropriately designate a jury or a trial judge as the final arbiter of whether a particular disclosure caused harm to the public interest in the context of adjudicating criminal guilt. Such individuals may not have an appropriate understanding or an appreciation of the possible impact of releasing that information, and will necessarily not be in a position to adequately assess how the disclosure of a particular piece of information may, when taken together with other information, cause prejudice or risk causing prejudice to security interests. In addition to creating a significant risk of suboptimal outcomes at trial, such a defence may also be unfair to members of juries as it places upon them a significant responsibility regarding national security and the safety of participants, in circumstances in which they may not have sufficient understanding or visibility of the relevant issues to discharge that responsibility. A specific public interest defence would further be inconsistent with the general policy intention of section 35P, as outlined above.

Exception—disclosure of information already in the public domain

Stakeholder suggestion

Some stakeholders have suggested that the offences are subject to an exception for the disclosure of information that is already in the public domain, on the basis that there can be no harm (or further harm) in subsequent disclosure or ‘re-publication’ of such information.

Comments

The offences in subsections 35P(1) and 35P(2) are intended to cover information that is already in the public domain. This reflects the fact that the significant risks associated with the disclosure of information about an SIO (including its existence, methodology or participants) are just as significant in relation to a subsequent disclosure as they are in relation to an initial disclosure. Limiting the offences to initial disclosures would create an arbitrary distinction between culpable and non-culpable conduct, on the basis of a technical question of the order in which multiple disclosures were made.
Consideration was given to the inclusion of a specific defence for the communication of information already in the public domain by reason of the authority of the Commonwealth. However, given that it is highly unlikely information about an SIO would ever be authorised, or capable of authorisation, for public release, it was considered that appropriate provision for such circumstances was made via the general defence of lawful authority under section 10.5 of the Criminal Code, together with general prosecutorial and investigative discretion. Further, there is no equivalent exception in the offences in sections 15HK and 15HL of the Crimes Act for information already in the public domain.

Proposed subsection 35P(3) does, however, contain a number of exceptions for permitted disclosures. These include, in paragraph (b), disclosures for the purposes of legal proceedings arising out of or otherwise related to the SIO scheme, or any report of such proceedings. This exception could therefore apply to a journalist who reported on legal proceedings in which the existence of an SIO was disclosed. (However, disclosure may further be subject to any protective orders the Court may make in relation to such evidence.)

**Repeal the basic offence in subsection 35P(1) (or repeal section 35P in entirety)**

**Stakeholder suggestion**

Some stakeholders have argued that the offences in section 35P should be limited to the aggravated offence in subsection 35P(2), because criminal sanctions should apply only to those disclosures that are intended to cause harm, or which actually result in harm, to the effective conduct of an operation or to the safety of participants or their families or associates. This was the subject of an amendment moved by the Australian Greens in the debate of the Bill in the Senate (and subsequently moved by the Australian Greens in the House of Representatives). The amendment was defeated in both chambers.

Some stakeholders have further suggested that the disclosure of information relating to an SIO should not be the subject of a specific criminal offence, because conduct constituting the offences in section 35P is already capable of being covered by other offences of general application. For example, the offences in section 79 of the Crimes Act for the unauthorised disclosure of official secrets, and the offences in section 92 of the ASIO Act for publishing the identity of an ASIO employee or an ASIO affiliate.

**Comments**

In response to the suggestion that section 35P should be limited to the aggravated offence in subsection 35P(2) and should not include the basic offence in subsection 35P(1), the Government has previously expressed the view that the retention of the basic offence is necessary and appropriate. As mentioned above,
the Government expressed support for the view, as also articulated by the ALRC in its 2009 report on secrecy laws, that secrecy offences in respect of intelligence-related information should not require proof of intent to cause harm, or resultant or likely harm, because such harm is implicit from the nature of the information disclosed.

In response to suggestions that there is no need to specifically criminalise disclosures of information relating to SIOs, the Government has previously expressed a view that specific criminal offences are needed to precisely target, denounce, penalise and deter the disclosure of information relating to special intelligence operations, which is of the most sensitive character. The offences in section 79 of the Crimes Act are of broader application to a range of official information, and carry lesser maximum penalties in recognition of this broader application. For example, the offence in subsection 79(2) of the unauthorised communication of official secrets with intent to prejudice the security or defence of the Commonwealth carries a maximum penalty of seven years’ imprisonment. Offences that do not require an intention to cause harm, such as that in subsection 79(3), carry a maximum penalty of two years’ imprisonment.

Further, we caution against the making of an assumption that the maximum penalties applying to the general secrecy offences in Part VII of the Crimes Act are necessarily remain adequate and appropriate in the contemporary security environment. Given recent international incidents involving the unauthorised disclosure of government information, there might be said to be a case to reconsider the existing maximum penalties applying to secrecy offences of general application, such as those in Part VII of the Crimes Act, to ensure that the offences remain appropriate and effective.

In addition, while the identity offences in section 92 of the ASIO Act carry a maximum penalty of 10 years’ imprisonment as a result of amendments made by the National Security Legislation Amendment Act (No 1) 2014, they do not adequately reflect the nature of the harm caused by unauthorised disclosures of information relating to an SIO. (Particularly prejudice to the operation, as distinct from to the lives, safety or livelihoods of participants, their families or associates.)

**Replace the fault element of recklessness with knowledge**

**Stakeholder suggestion**

Some stakeholders have argued that the offences should only apply to persons who make a disclosure, knowing that the information disclosed related to an SIO. It was asserted that the fault element of recklessness is an unduly low bar, as the mere fact of ASIO’s involvement or suspected involvement could be sufficient to establish a person’s awareness of a substantial risk that the information related to an SIO.
Comments

The Attorney-General’s correspondence to the Senate Scrutiny of Bills Committee provided the following summary of the Government’s position that it would not be appropriate to apply a fault element of knowledge of the circumstance that the information related to an SIO (a copy is enclosed in the volume of materials accompanying this briefing):

The physical element in (b) of each of ss 35P(1) and (2) is a circumstance in which conduct occurs, within the meaning of s 4.1.1(c) of the Criminal Code 1995. As the provision does not specify a fault element, s 5.6(2) of the Criminal Code operates to provide that the fault element of recklessness applies. Recklessness is defined in s 5.4(1) of the Criminal Code to mean that the person was aware of a substantial risk that the information disclosed related to a special intelligence operation, and unjustifiably, in the circumstances known to him or her at the time, took the risk of making the disclosure.

Accordingly, it is not necessary for the prosecution to establish that a person had knowledge that the information related to an SIO, in the sense of a conscious awareness of the existence of an SIO and that the relevant information related to that operation. However, the prosecution must establish, beyond reasonable doubt, that a person was aware of a real and not remote possibility that the information was so related. As such, the offences will not apply to a person who disclosed information entirely unaware that it could relate to an SIO, since there would be no evidence of an advertence to a risk of any kind.

In addition, proof of a person’s awareness of a substantial risk will depend on the availability of evidence of a person’s awareness of relevant information about an operation or a suspected operation, which must suggest more than mere advertence to a nominal or speculative possibility that an SIO might have been declared, and that the information proposed to be communicated related to that operation. Rather, the prosecution would need to prove, beyond reasonable doubt, that the person was aware of a real and not remote possibility that the information related not just to an intelligence or national security related operation of some general description, but specifically to an SIO.

As the Committee has observed, SIO authorisations are an entirely internal matter. This means that the burden on the prosecution to prove, to the criminal standard, that a person was advertent to a risk that a specific circumstance existed, and that that risk was significant, is an onerous one.

In addition to providing a person was aware of a substantial risk that the relevant circumstance existed, the prosecution must further prove that, having regard to the circumstances known to the person at the time of making the disclosure, it was unjustifiable to have taken that risk. The actions of a person in attempting to manage risk are directly relevant to an assessment of whether a person’s actions were
justifiable. For example, the actions of a journalist in attempting to check facts and consult with ASIO about any possible concerns in reporting on a matter would tend very strongly against a finding that such a person had acted unjustifiably in the circumstances. As such, adherence to the usual practices of responsible journalism in the reporting of operational matters relating to national security is directly relevant to the question of whether a communication was justified in the circumstances.

The policy justification for adopting recklessness, rather than knowledge, as the applicable fault element is ... that the wrongdoing targeted by proposed s 35P is that the disclosure of information about an SIO will, by its very nature, create a significant risk to the integrity of that operation and the safety of its participants. The fault element of recklessness gives expression to the policy imperative to deter such conduct by clearly placing an onus on persons contemplating making a public disclosure of such information to consider whether or not their actions would be capable of justification to the criminal standard. In the event that there is doubt, and the proposed disclosure relates to suspected wrongdoing by ASIO, consideration should be given to making an appropriate internal disclosure, such as to the Inspector-General of Intelligence and Security, or to the Australian Federal Police if the commission of a criminal offence is suspected.

Statutory sentencing considerations—public interest

Stakeholder suggestion

In the debate of the Bill in the Senate, independent Senator for South Australia Nick Xenophon moved amendments to section 35P, which would require a sentencing court to take account of whether or not, to the knowledge of the court, the disclosure was in the public interest.

Comments

The Attorney-General did not support this amendment when moved in the Senate on 25 September 2014. The Attorney-General remarked, at p. 7247 of Senate Hansard:

The government does not support the amendment because it is entirely unnecessary. The amendment proposes that the following words be added to section 35P:

A court must, in determining a sentence to be passed or an order to be made in respect of a person for an offence against subsection (1), take account of whether or not, to the knowledge of the court, the disclosure was in the public interest.

Senator Xenophon, that is what courts would always and routinely do in a case of this kind. If a person were to be prosecuted and convicted of an offence of this kind and there was material before the court that enabled his counsel to urge on the sentencing judge that he was acting in the public interest, it is inconceivable that that consideration
would not be had regard to as a potential circumstance of mitigation. The principles of criminal sentencing are a very, very, very well established discipline and the amendment you have proposed instructs by statute a court to do what a court always would do and since time immemorial has always done. So the government does not support the amendment because it is entirely unnecessary.

However, having regard to the concerns you have raised I have amended the explanatory memorandum to refer to the Prosecution Policy of the Commonwealth, which actually explicitly indicates that public interest is a factor to be had regard to in relation to a decision to prosecute. So I spoke about a judge considering a sentence in relation to a convicted person; but at a prior stage in the process it is also, under the existing Prosecution Policy of the Commonwealth, a matter to which a prosecutor must have regard in exercising a prosecutorial discretion.

Finally ... as I pointed out before ... this provision does not take the law of the Commonwealth any further than it already stands. Under [sections 15HK and 15HL] of the Crimes Act the same provisions apply, and have applied since 2010, to controlled operations by the Australian Federal Police. This provision merely applies the same regime as applies to controlled operations by the Australian Federal Police to special intelligence operations carried out by ASIO.

Sunset provisions and review requirement

Stakeholder suggestion

Some stakeholders have argued that the provisions of Division 4, including section 35P, should sunset after a specified period of operation, such as five years. This was said to be in recognition of the ‘exceptional’ nature of the scheme, which was said to warrant Parliament’s further assessment of the effectiveness and continued necessity of the scheme after some operational experience has been acquired.

Comments

AGD and ASIO made the following remarks in a joint submission to the PJCIS inquiry into the (then) Bill (a copy of which is provided in the accompanying volume of materials):

The Department and ASIO do not support the application of a sunset provision to the provisions in Schedule 3 to the Bill. The need to provide participants in covert intelligence operations with limited protection from legal liability is not temporary in nature. Rather, its ongoing availability is needed to ensure that the Organisation has the capacity to meet emerging and future security challenges, by ensuring its capacity to gain close access to persons and groups of security concern, and providing legal certainty to persons assisting the Organisation in the performance of its functions.
The permanent nature of a special intelligence operations regime is consistent with the controlled operations scheme in Part 1AB of the Crimes Act, and the immunity from liability conferred upon staff members and agents of Intelligence Services Act agencies under section 14 of that Act. Both of these measures were enacted without sunset clauses, and this was found acceptable to the Parliament in 2010 and 2001 respectively.

AGD and ASIO went on (in Submission 8 to this inquiry) to indicate some possible ways forward in relation to section 35P. These were provided on the basis that (subject to one suggested amendment, described in the second dot point below), there is a satisfactory policy justification for retaining the offences. These were, in brief, as follows:

- Retain the status quo, subject to ongoing INSLM review.
- Insert a general statutory prosecutorial consent requirement in section 35P (seemingly referring to consent on the part of the Attorney-General).
- Possible consideration of targeted amendments to the physical elements.
- Possible limitations on the type of information subject to the offences.
- Possible time limit (for example, a decade or decades) on non-disclosure periods.
Appendix G—A selection of comments about oversight and the role of the IGIS in submissions to the inquiry

Several submissions commented on the fact that oversight of the activities of intelligence agencies including ASIO in Australia was relatively weak by comparison with other comparable countries. In this context, it was submitted (in very broad summary form) that:

- The United States, Canada and the United Kingdom in particular have more judicial scrutiny of the activities of intelligence agencies because certain relevant rights and freedoms (such as freedom of expression) are constitutionally entrenched or specifically protected under legislation which provides for associated legal remedies:
  - In the United States, some aspects of the activities of intelligence agencies are also overseen by the Foreign Intelligence Surveillance Court (notwithstanding that the Court operates largely in secret and is quite constrained in practice in its ability to test information put to it or to enforce compliance with its judgements).
  - New Zealand also has specific human rights laws but, as in Australia, the protection of human rights does not generally involve associated legal remedies and is subject to legislative override.

- The United States and Germany have more legislative scrutiny of the activities of intelligence agencies because relevant legislative committees have more power than does the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in Australia:
  - in accordance with section 29 of the Intelligence Services Act 2000, the PJCIS is limited, generally, to reviewing the administration and expenditure of relevant intelligence agencies
  - in the United States, the Intelligence Committees and the Judiciary Committees in the Senate and the House of Representatives exercise general oversight over intelligence collection programs and are briefed regularly, and
  - in the case of Germany, legislative scrutiny is supported by other bodies such as the G10 Commission appointed to this end (and the G10 Commission monitors and authorises requests for surveillance activities subject to the G10 law).
While the Inspector-General of Intelligence and Security (IGIS) is an important element of the scrutiny of the activities of relevant intelligence agencies in Australia and has considerable powers, the IGIS:

- is an arm of the executive and maintains quite strict secrecy
- has functions which are limited (put broadly) to reviewing the lawfulness and propriety of the activities of relevant intelligence agencies:
  - the IGIS does not, for example, necessarily contest the Government’s view of the law, including international law, and
- may need further resources given the various and expanding range of functions required to be performed.

The IGIS also provided a submission to the inquiry. This states, in relation to the general oversight role of the IGIS, that:

The Office of the IGIS is situated within the Prime Minister’s portfolio. The IGIS is not subject to direction from the Prime Minister, or other ministers, on how responsibilities under the Inspector-General of Intelligence and Security Act 1986 (the IGIS Act) should be carried out. The Office is not part of the Department of the Prime Minister and Cabinet and has separate appropriation and staffing.

The IGIS Act provides the legal basis for the IGIS to conduct inspections of the intelligence agencies and to conduct inquiries of the Inspector-General’s own motion or at the request of a Minister.

The overarching purpose of IGIS’s activities is to ensure that each intelligence agency acts legally and with propriety, complies with ministerial guidelines and directives, and respects human rights. A significant proportion of the resources of the office has in the past been directed towards ongoing inspection and monitoring activities, so as to identify issues, including about the governance and control frameworks within agencies, before there is a need for major remedial action. OIGIS staff have access to all documents of the intelligence agencies and the IGIS is often proactively briefed about sensitive operations.

The inspection role of the IGIS is complemented by an inquiry function. In undertaking inquiries the IGIS has strong investigative powers, including the power to require any person to answer questions and produce relevant documents, take sworn evidence, and enter agency premises. IGIS inquiries are conducted in private because they almost invariably involve highly classified or sensitive information, and the methods by which it is collected. Conducting an inquiry is resource intensive but
provides a rigorous way of examining a particular complaint or systemic matter within an agency.

In relation to oversight of the SIO scheme, the IGIS submission states that:

A number of provisions in the ASIO Act in relation to SIOs are designed to facilitate oversight of SIOs by my office.

- ASIO is required to notify the IGIS when an SIO is approved by the Attorney-General.
- ASIO must also provide a report to the Attorney-General and to the IGIS after six months, and at the conclusion of an SIO.
- The section 35P offence for unauthorised disclosure contains exceptions to enable disclosure of information that could reveal details of an SIO to be made to an IGIS official.

I have established an inspection program to provide oversight of ASIO’s use of SIOs. At present, my staff will inspect each SIO that is approved by the Attorney-General, and this oversight will cover the full duration of each SIO. As with all IGIS inspections, my staff will have access to all documents relating to an SIO and the purpose of the inspection is to consider whether the SIO is conducted with legality, with propriety and with due regard to human rights. The inspection will have regard to the SIO authorisation documentation as well as any activities undertaken in reliance on the authorisation.

As noted above, the IGIS’s role is to consider issues of both legality and propriety. My staff look at whether ASIO complies with relevant legislation as well as the Attorney-General’s Guidelines, made under section 8A of the ASIO Act. Among other things, the Guidelines include a requirement of proportionality—that is that any means used for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence. Additionally, we also consider ASIO’s compliance with any relevant internal policies, and I may engage in dialogue with ASIO should I feel that there is a need for greater guidance to be provided to staff in relation to particular matter.

... Where issues are identified in inspections my usual practice is that they are raised with relevant senior officers and reported to the Director-General of Security. Should serious concerns arise, I may consider it appropriate to advise the Minister responsible for ASIO and/or the Prime Minister.
IGIS provides an Annual Report to Parliament each year. While there will be limits on what can be said in an unclassified report, it is my usual practice to comment on inspection activities, including noting whether any issues of legality or propriety have been identified.

In addition to regular inspections, my office investigates complaints and conducts formal inquiries under section 9 of the IGIS Act. Inquiries may be conducted of the Inspector-General’s own motion, in response to a complaint or at the request of the relevant Minister or the Prime Minister. IGIS also has a role under the Public Interest Disclosure Act 2013 (PID Act) to receive authorised disclosures in relation to the Australian intelligence agencies. The PID scheme protects the confidentiality of disclosers and provides statutory protections against reprisals.

Any person may make a complaint to my office under the IGIS Act. It is not restricted to employees or agents of the intelligence agencies, and could include a member of the public or journalist who had concerns about the activities of an intelligence agency. Should my office receive a complaint about an SIO, or conduct that may be related to an SIO, this would be taken very seriously. Section 11 of the IGIS Act provides that where a complaint is made to the IGIS in respect of action taken by an intelligence agency and the matter is within the IGIS’ functions, the IGIS shall, subject to certain considerations, inquire into the action.

... There are also strong secrecy provisions in section 34 of the IGIS Act, which protect information provided by a complainant from unauthorised disclosure by the IGIS or IGIS staff. The secrecy provision extends to preventing information being disclosed to or compelled by a court, offering the complainant significant confidentiality in respect of any information they provide to my office.

The IGIS is correct in pointing out that the office is a statutory and independent one and not part of the executive. An assessment of the criticisms of the IGIS Act is beyond the scope of this report.
Appendix H—Brief history of ASIO and the ASIO Act

This Appendix deals with ASIO and the history of ASIO secrecy, before and after the ASIO Act was enacted in 1979, including relevant parts of the Hope Royal Commission reports which preceded and followed that enactment. Appendix L provides a broader historical context surrounding relevant secrecy offences.

ASIO established

ASIO was established on an executive basis by Prime Minister Chifley on 16 March, 1949.

Secrecy was governed initially administratively (by employment conditions) and by the general secrecy offences in the Crimes Act.

ASIO sought legislative support from the outset to protect Australia against various security threats and was concerned that Australia needed offences relating to secret information falling short of espionage.

ASIO placed on a statutory basis

The Australian Security Intelligence Organization Act 1956 (the 1956 Act) placed ASIO on a statutory basis. This Act set out ASIO’s functions and broad employment framework.

The 1956 Act did not contain an ASIO-specific secrecy provision.

However, section 15 of the 1956 Act provided that the Director-General and officers and employees of ASIO shall be deemed to be ‘Commonwealth officers’ for the purposes of the Crimes Act 1914 (Crimes Act)—section 91 of the ASIO Act now makes corresponding provision. This section ensured that sections 70 and 79 of the Crimes Act (offences relating to disclosures of what might be termed ‘official information’ and disclosures of what are called ‘official secrets’, respectively) applied to such persons.
The First Hope Royal Commission

In 1974 the Australian Government established the Royal Commission on Intelligence and Security (‘the RCIS’, also known as ‘the First Hope Royal Commission’), which was conducted by Justice Robert Hope.36 The terms of reference for the RCIS required a broad-ranging inquiry into the past activities, and recommendations for reform, of Australia’s security and intelligence agencies. For ASIO, the focus was on improving accountability, including in terms of ministerial accountability and financial management. The RCIS was the principal catalyst for the current ASIO Act.

The RCIS recognised the need for ASIO to maintain secrecy surrounding its activities. This was evident in the recommendations and the manner in which the RCIS itself was conducted (largely privately rather than publicly) and reported (with sections redacted).

For example, Part IV of the ASIO Act deals with ‘security assessments’, a form of advice about security that ASIO provides to government bodies relating to certain administrative action. In accordance with RCIS recommendations, many security assessments are subject to administrative review on the merits by an independent tribunal, initially the Security Appeals Tribunal, subsequently the Administrative Appeals Tribunal (AAT). There are, nonetheless, various special rules and procedures in Part IV of the ASIO Act and in the Administrative Appeals Tribunal Act 1975 (AAT Act) that attach to the notification and review of security assessments. These are designed, broadly, to ensure that notification and review of security assessments does not prejudice security.

One aspect of the security assessment regime involves assessing whether people should be given access to information, access to which is controlled or limited on security grounds (for example, highly security-classified information). Such assessments relate to the fitness of persons to be so-called ‘trusted insiders’, so far as access to such information is concerned.

The December 1984 Report on the Australian Security Intelligence Organization, part of the Royal Commission into Australia’s Security and Intelligence Agencies

---

36 The Commission was established by the incoming Whitlam Labor Government after a long period in Opposition. The parliamentary debates indicate deep concerns among various Members of Parliament about the activities and accountability to the Government of the intelligence agencies, particularly ASIO and its role during the Cold War (including the events dealt with by the Petrov Royal Commission in 1954).
(‘the RCASIA’, also known as ‘the Second Hope Royal Commission’) reconsidered this aspect of security assessments. In this context (specifically, the question whether such security assessments should involve matters going to a person’s reliability, as well as to the person’s loyalty) Justice Hope commented that:

The disclosure of secrets or the exposure of secure areas to risk through inadvertence or carelessness can result in just as much damage to the national interest as can result from espionage or sabotage.

One of the most important justifications of secrecy relates to the need to protect capability and the flow of information from ASIO human sources.

The RCIS discussed the importance of human sources to ASIO’s work and specifically, the need to protect the identity of agents (Fourth Report, Vol I, paragraphs 173–182). The RCIS did not, in that report, specifically recommend a specific secrecy offence relating to protecting the identities of ASIO agents.

The following extract from *Spy Catchers: The Official History of ASIO* (published in 2014, Appendix: Protecting the Identity of ASIO Agents, pages 563–570, footnotes omitted) describes the significance of human sources to ASIO, along with relevant aspects of ASIO’s history including relevant aspects of the RCIS:

Following its establishment on 16 March 1949, ASIO developed a network of sources. Some of these were technical, such as telephone intercepts or listening devices, but the majority were people—of different age, class, ethnicity, occupation, religion, sex and motivation. People are useful sources of intelligence because they can provide information that is unobtainable by any other means. People, for instance, can elicit information, perhaps by influencing a target to disclose or discuss a particular issue, in a way that technical aids cannot. For its own internal purposes, ASIO divides its human sources into ‘agents’ and ‘contacts’. The differentiation is sometimes blurred, but generally, the former refers to people who are directed and controlled—or briefed—by an ASIO officer (employee) to penetrate a target, whether it be a group or an individual, while the latter provides information of their own accord rather than under a brief or ASIO control. In practice, although not a steadfast rule, only agents receive money for their services.

The important role that agents have played in the security of Australia has largely been overshadowed by the disdain for the ‘dobber’ in Australian society. Justice Robert Marsden Hope, who undertook a number of royal commissions into Australia’s intelligence agencies, recognised this. ‘There is in Australia some feeling of antagonism towards agents,’ he wrote, ‘based ... on the deception that is involved. An agent has to be accepted by the persons about whom he is reporting as
one of their number, and as sympathetic to their objectives. In fact he is not own of their number, and may not be sympathetic to their objectives’.

Agents, particularly successful ones, often had to assume a role, usually at odds with their political and ideological beliefs, maintain that covert role around their families, friends and colleagues, and live with the consequences ... That the stresses of being an agent were high—and difficult—cannot be doubted. Neither can agents’ sense of service and contribution to Australia’s security. Whatever one’s opinion of informants, Justice Hope concluded that ‘a security organisation could not perform its functions adequately without making use of people who are prepared to take on such a role’.

**Source protection**

Building on one of the most basic practices of intelligence agencies, source protection has been uppermost in the minds of ASIO since its inception. The ‘primary purpose’ of this protection, according to a classified ASIO manual, was ‘to preserve ASIO’s continuing access to the information or assistance which such persons can provide’. In other words, source protection is fundamental to the continued flow of intelligence, and to ensure that future agents are not put off from providing information to ASIO in the fear that their identities may one day be exposed. Of equal importance to ASIO, adequate measures were taken ‘to protect [agents] from harm to their career and/or their personal or physical well-being’ that might arise were their role to be disclosed. Although the current penalty for revealing the identity of an ASIO agent is one year’s imprisonment, there was no legal protection for ASIO’s agents, or indeed its officers, for ASIO’s first 30 years. Anonymity of agents’ identities could therefore only be preserved through best practice. This meant that from its very beginning, ASIO had to build and rely upon its own security systems for source protection.

While ASIO could regulate its own security procedures, it had no control over what might be asked publicly. It did, however, sometimes offer suggestions as to what stance the Government could take to protect ASIO’s interests ... Such warnings often led to the common statement that both ASIO and the Government would ‘not comment’ on security issues and would ‘neither confirm nor deny’ matters of national security, including agents’ identities.

Such statements still did not provide any legal protection. The Royal Commission on Intelligence and Security, regarded as a turning point in ASIO’s history, recognised this absence. ‘Because agents are of such importance to the performance of the functions of a security organisation, it is critical to the organization that their identity is protected’, it argued. Confirming ASIO’s long-held views, it continued:
If an agent’s identity is disclosed his access to the target organization or person is likely to be closed. He will be embarrassed if not endangered, and breach of his confidence with ASIO is likely to cause him to cut his ties with ASIO even if he could be of further use to it. Other sources who learn that an agent has been blown may cut their ties with ASIO. Potential sources may be deterred.

Legal protection came two years later with the *Australian Security Intelligence Organisation Act 1979*. Today, citing Section 33 of the *Archives Act 1983*, ASIO continues to protect the identities of its sources by redacting material that might otherwise reveal their role from files transferred to the National Archives of Australia. It is an important protection and it is only in rare circumstances that an exception is made to the rule.

The RCIS recommended an ASIO-specific secrecy offence (a principal justification for what became section 18 of the ASIO Act) in relation to certain disclosures made by ‘insiders’.

The background to the establishment of the RCIS involved a range of allegations of misuse of security intelligence and information by ASIO. The RCIS discussed the collection and dissemination of security intelligence in some detail and made a related recommendation. The following extract from the Fourth Report of the RCIS contains part of that discussion and the relevant recommendation (it is interesting to note that the recommended provision was designed in part to protect the interests of individuals, not simply as an aid to secrecy as such).

(e) Intelligence dissemination

(i) The discretion to communicate security intelligence

222. Intelligence is not collected to establish a library. Its collection is only justified by its use. Decisions as to its use are important and at times difficult. Much intelligence may only be relevant, or may be primarily relevant, to ASIO itself. Other intelligence, however, to be exploited in the interests of security, must be communicated to other persons. Great difficulty lies in determining when and to whom it is proper to communicate intelligence, and in establishing proper safeguards to ensure that it is not communicated otherwise.
(ii) Unauthorized or improper disclosure

226. The Act itself contains no express provision prohibiting the unauthorised or improper communication of intelligence, and imposes no penalties in this regard. The intelligence held by ASIO about individuals is often highly prejudicial to them, and its dissemination should be strictly controlled by legislation as well as by ethical rules. The minimum rules which should be contained in the legislation are that the communication may only be made by the DG or by somebody authorized by him, either generally or in the particular matter; and that the communication of any intelligence by an unauthorized person, or otherwise than for the purposes of the Act, should be prohibited. Persons who infringe these provisions or who authorize its infringement should be subject to severe penalties.

... 

228. People to whom ASIO disseminates intelligence should be under an obligation not to disseminate it further except on a strict need-to-know basis and for the purpose of implementing security. In appropriate cases, the person should be required to return to ASIO the document containing the information after he has used it for the purposes it was supplied.

...

Dissemination of security intelligence

768. Insertion of provisions to control the dissemination of security intelligence, and to prohibit improper or unlawful communication of such information, including provisions that:

(a) The communication of intelligence shall be made only by the Director-General or by someone authorized by him.

(b) The communication shall not be made except for a purpose relevant to security.

(c) The communication of any intelligence by an unauthorized person shall be prohibited.

(d) Infringement of these provisions to be subject to severe penalties (para 226).
The ASIO Act

The *Australian Security Intelligence Organization Act 1979* (ASIO Act) superseded the 1956 Act and commenced on 1 June 1980.

Section 18 implemented the recommendation made by the RCIS in relation to dissemination of security intelligence. However, section 18 did, and still does, permit the communication in certain circumstances of ASIO information that is not ‘intelligence relevant to security’. As the Explanatory Memorandum to the ASIO Bill states:

> ... Because para 17(1)(b) in effect excludes from the functions of the Organization the communication of intelligence for purposes not relevant to security and the Organization may, in the course of performing its ordinary functions, come into possession of information that, while not relevant to security, is relevant to the detection or prevention of serious crimes and other matters, sub-clause (3) provides that, in the limited cases there set out, information may be communicated for non-security purposes.

The reference to legal protection for human sources in the earlier extract from *The Spy Catchers* refers to section 92 of the ASIO Act, an original provision of the Act. Section 92 made provision in respect of officers and employees of ASIO, as well as ASIO agents—the latter (specifically, human sources) having been the focus of attention in the RCIS. (Put broadly, section 92 now prohibits a person from making public the identity of ASIO employees and ASIO affiliates, and certain other persons associated with them.)

The reference in the same extract to the current penalty being imprisonment for one year is out of date—the Act, which added section 35P to the ASIO Act (post-dating the publication of *Spy Catchers*), increased the penalty for an offence against section 92 to imprisonment for 10 years.

Of interest in the context of the present inquiry, the Opposition at the time proposed an amendment of clause 92 in the Parliament (which was rejected) along the lines that the required consent of the Attorney-General to any prosecution of a person for an offence against section 92 be provided only where the Attorney-General was satisfied that the actions of the relevant person have, or would be likely to have, the effect of:

- endangering the physical safety of the officer, employee or agent of the Organisation, or
...seriously prejudicing security.

The Opposition at that time considered that including such matters in the offence itself might create difficulties of proof (which may still be true, but there are now additional statutory mechanisms to protect national security information). In part, the justification for the suggested amendment echoes some of the concerns expressed in relation to section 35P (Hansard, Senate, 10 May 1979 at 1859, Senator Evans):

It is crucially important that the abuse or misuse of ASIO power ought to be able to be made public. The language of this clause ought not to be drawn in such a way that it operates in a catch-all fashion, including within its potential ambit a whole variety of forms of disclosure; including the well-motivated, the innocent and the positively beneficial in the interests of the community as a whole, as well as those of a more sinister motivation.

The Government rejected the suggested amendment, principally on the basis that there was no sufficient justification, or apparent precedent, for restricting the matters which the Attorney-General might want to consider in deciding whether to consent to a prosecution.

For completeness, the ASIO Act also contained section 81, a secrecy offence applicable to members and certain staff of the Security Appeals Tribunal (now to the members and certain staff of the Administrative Appeals Tribunal) in connection with the Tribunal’s role in providing independent review of security assessments. Such a provision means that such persons need not be treated as ASIO insiders for section 18 purposes, which may be important to the independence of the relevant tribunal.

The Second Hope Royal Commission

The RCASIA Report referred to earlier discussed the assessment and communication of intelligence. The Commission recommended some reform of section 18 (in particular, of the capacity to communicate incidental intelligence, being an exception to the section 18(2) offence)\(^\text{37}\).

Section 18 was amended by the Australian Security Intelligence Organization Amendment Act 1986 (No 122 of 1986) to implement these recommendations to

\(^\text{37}\) See Chapter 8 of the RCASIA Report on the Australian Security Intelligence Organization, December 1984, in particular, paragraphs 8.73-8.89.
some extent. Further amendments have since been made and sections 18(3)-(4B) now provide for and in relation to such communications.

The RCASIA Report makes the following comments (paragraph 17.45) in connection with a recommendation that the Director-General consider acknowledging publicly the identities of more of the senior officers of ASIO.

... Section 92 of the ASIO Act makes it an offence publicly to identify an employee or agent of ASIO or of a person connected with such an employee or agent. There are good security reasons for protecting the identities of some, but not necessarily all, ASIO officers. Corresponding provisions in the Canadian Security Intelligence Service Act (s.18) and the United States Intelligence Identities Protection Act of 1982 are related more clearly to people with an operational need for anonymity.
Appendix I—ASIO public accountability

Freedom of information

Section 3 of the *Freedom of Information Act 1982* (FOI Act) relevantly provides that:

- the objects of the Act are to give the Australian community access to information held by the Government of the Commonwealth by:
  - requiring agencies to publish the information
  - providing for a right of access to documents, and
- the Parliament intends, by these objects, to promote Australia's representative democracy by contributing towards:
  - increasing public participation in Government processes, with a view to promoting better-informed decision-making
  - increasing scrutiny, discussion, comment and review of the Government's activities, and
- the Parliament also intends, by these objects, to increase recognition that information held by the Government is to be managed for public purposes, and is a national resource, and
- the Parliament also intends that functions and powers given by this Act are to be performed and exercised, as far as possible, to facilitate and promote public access to information, promptly and at the lowest reasonable cost.

ASIO is an ‘exempt agency’ for the purposes of the FOI Act: see section 7(1) and Division 1 of Part I of Schedule 2.

Other agencies are exempt from the operation of the FOI Act in relation to a document that has originated with, or has been received from, ASIO: see section 7(2A) of the FOI Act.

Privacy

Section 2A of the *Privacy Act 1988* (Privacy Act) provides that the objects of the Act are to:

- promote the protection of the privacy of individuals
- recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities
- provide the basis for nationally consistent regulation of privacy and the handling of personal information
• promote responsible and transparent handling of personal information by entities
• facilitate an efficient credit reporting system while ensuring that the privacy of individuals is respected
• facilitate the free flow of information across national borders while ensuring that the privacy of individuals is respected
• provide a means for individuals to complain about an alleged interference with their privacy, and
• implement Australia's international obligation in relation to privacy.

ASIO is effectively exempt from the Privacy Act: see section 7(1)(a)(i)(B) and section 7(2)(a) of the Act, together with related definitions.

Ombudsman

The Ombudsman, established by the Ombudsman Act 1976 (Ombudsman Act), investigates complaints about Commonwealth administration and has other functions in relation to Commonwealth administration generally, including in relation to public interest disclosures.

ASIO is effectively exempt from the Ombudsman Act: see the definition of ‘prescribed authority’ in section 3 of the Act, and regulation 4 of, and Schedule 1 to, the Ombudsman Regulations 1977.

The Archives

Section 2A of the Archives Act 1983 (Archives Act) provides that the objects of the Act are:

• to provide for a National Archives of Australia, whose functions include:
  – identifying the archival resources of the Commonwealth
  – preserving and making publicly available the archival resources of the Commonwealth
  – overseeing Commonwealth record-keeping, by determining standards and providing advice to Commonwealth institutions, and
• to impose record-keeping obligations in respect of Commonwealth records.

ASIO is the subject of special treatment under the Archives Act: see sections 27–29. Many ASIO records would be ‘exempt records’ (see section 33) for the purposes of the provisions of the Archives Act, which provide for access to Commonwealth records.
Public interest disclosures

The Public Interest Disclosure Act 2013 (PID Act) is a key accountability mechanism given the context of this inquiry—many submissions to the inquiry assert the need for suspected serious wrongdoing by ASIO to be able to be reported, in the public interest.

The aims of the PID Act, set out in section 6, are to:

- promote the integrity and accountability of the Commonwealth public sector
- encourage and facilitate the making of public interest disclosures by public officials
- ensure that public officials who make public interest disclosures are supported and are protected from adverse consequences relating to the disclosures, and
- ensure that disclosures by public officials are properly investigated and dealt with.

The PID Act provides for various forms of protection of current and former public officials who make ‘public interest disclosures’. These protections are expressed generally to have effect despite other Commonwealth laws (see section 24) — relevantly including Commonwealth secrecy offences. Section 26 provides for what amount to ‘public interest disclosures’. The requirements attached to making an ‘external disclosure’ include, among other things, that:

- the information tends to show, or the discloser believes on reasonable grounds that the information tends to show, one or more instances of ‘disclosable conduct’:
  - ‘disclosable conduct’ is defined in section 29 and section 33 provides that, despite section 29, conduct is not ‘disclosable conduct’ if it is:
    - conduct that an intelligence agency engages in in the proper performance of its functions or the proper exercise of its powers, or
    - conduct that a public official who belongs to an intelligence agency engages in for the purposes of the proper performance of its functions or the proper exercise of its powers
• the information does not consist of, or include, ‘intelligence information’:
  – ‘intelligence information’ is defined broadly in section 41 as (among other things):
    ▪ information that has originated with, or has been received from, an ‘intelligence agency’ (for example, ASIO)
    ▪ information that is about, or that might reveal ‘intelligence agency’ sources, methods or operations
    ▪ information received from a foreign government agency with functions similar to an ‘intelligence agency’ and that is about, or that might reveal, a matter communicated by that authority in confidence
    ▪ ‘sensitive law enforcement information’ (as defined)\(^{38}\)
• none of the conduct with which the disclosure is concerned relates to an ‘intelligence agency’:
  – the section 8 definition of ‘intelligence agency’ includes ASIO.

In relation to ASIO, it follows that a ‘public interest disclosure’ may be made internally (to an ‘authorised internal recipient’ as defined) or to the Inspector-General of Intelligence and Security (see sections 43 and 63 and other provisions relating to an ‘investigative agency’). The PID Act does not provide protection to public officials who make external disclosures that consist of, or include, intelligence information, or that relate to the conduct of an intelligence agency, such as ASIO.\(^{39}\)

---

\(^{38}\) Even though there may be some overlap of information which cannot be the subject of a protected disclosure, the PID Act generally allows more scope for protected disclosures to be made in relation to the AFP than in relation to ASIO.

\(^{39}\) In this respect, the PID Act has been criticised by some commentators. Dr AJ Brown, for example, argues that the definition of ‘intelligence information’ is so broad as to effectively remove public disclosure as an option under the PID Act for intelligence agency officials (even, perhaps, in the context of an ‘emergency’ disclosure). He argues that a tighter definition of ‘intelligence information’ should be devised and that it is questionable whether the blanket carve-out legislated for in respect of intelligence agencies would meet constitutional tests of proportionality, if challenged on constitutional or rights-protection grounds—see Towards ‘Ideal’ Whistleblowing Legislation? Some Lessons from Recent Australian Experience, E-Journal of International and Comparative Labour Studies Vol 2 No 3 September-October 2013, 153–182.
Judicial review

Judicial review involves courts deciding whether administrative action has been taken lawfully, including that lawful procedures have been followed. Provided that is the case, judicial review is not generally concerned with which decision, among the range of possible lawful decisions, is in fact taken in any particular case. In other words, judicial review is not concerned with the merits of the decision.

The Administrative Decisions (Judicial Review) Act 1977 (ADJR Act) was intended to provide a simpler and more accessible form of judicial review than the common law. ASIO is effectively exempt from the ADJR Act: see paragraph (d) of Schedule 1 to the ADJR Act, which sets out classes of decisions to which the Act does not apply.

However, ASIO and its activities are not exempt, as such, from judicial review: see the decision of the High Court in Church of Scientology v Woodward (1982) 154 CLR 25, which dealt with and rejected various arguments to the effect that ASIO was immune from judicial review.

Further, the jurisdiction of the High Court under section 75 of the Constitution cannot be excluded by legislation.40 The Federal Court has an equivalent jurisdiction under section 39B of the Judiciary Act 1903.

Independent merits review

The Administrative Appeals Tribunal Act 1975 (AAT Act) provides for review of administrative decisions ‘on the merits’ by an independent tribunal—the Administrative Appeals Tribunal (AAT)—where those decisions are identified by legislation as being reviewable by the AAT. The extent to which ASIO is subject to administrative review by the AAT is both quite limited and the subject of special rules.

40 Chapter 3 of Administrative Review Council Report No 50, Federal Judicial Review in Australia (2012) (paragraphs 3.1–3.46), explains the evolution and nature of what is now called ‘constitutional judicial review’ by the High Court, including important recent jurisprudence. Constitutional judicial review is founded on the prerogative writs, and turns on the concept of ‘jurisdictional error’, based on the constitutional separation of powers.
In relation to ASIO, the AAT may only review:

- certain security assessments (see sections 54 and 36 of the ASIO Act and section 27AA of the AAT Act), of which notice must generally be given, subject to special rules set out in Part IV of the ASIO Act and in the AAT Act, and

- certain decisions taken under the Archives Act affecting ASIO records.
Appendix J—Relevant constitutional and international law

Constitutional law

For a Commonwealth law to be valid, the Parliament must have power under the Australian Constitution to make the law, and the law must otherwise be consistent with the Constitution.

Power to make the law

Section 51 of the Constitution provides that the Parliament has power, subject to the Constitution, to make laws with respect to certain matters (‘heads of power’). One ‘head of power’ that would provide broad support for section 35P is the power of the Parliament to make laws with respect to ‘the naval and military defence of the Commonwealth and of the several States, and the control of the forces to execute and maintain the laws of the Commonwealth’ (the defence power).

The defence power is a ‘purposive’ power. As such, to fall within the defence power, legislation must be capable of being regarded as appropriate and adapted for the purpose of defence. The defence power is not limited to actual armed conflicts—it is a broad power which enables laws to be made to facilitate preparedness for future conflicts and which ‘waxes and wanes’ according to the existence or absence of actual or imminent national threats, including acts of terrorism.41

While section 35P is cast in broad terms, the information to which it applies must at least ‘relate to’ a ‘special intelligence operation’ (SIO), which is a particular operational form of ASIO activity. The role of ASIO under the ASIO Act (very broadly) is to protect Australia and the people of Australia from various specified threats. There seems little reason to doubt that section 35P would be supported by the defence power.42

41 See, in particular, Thomas v Mowbray (2007) 233 CLR 307, a decision of the High Court in relation to the defence power and the control order regime established by Division 104 of the Criminal Code.

42 Note that Submission 36, from the Faculty of Law at Bond University asserts that because section 35P(1) of the ASIO Act prevents the disclosure of information which ‘relates to’ an SIO and which may have no negative impact on defence or any intelligence operation it is not supported by the defence power, and that it breaches the implied freedom of political communication.
**Implied freedom of political communication**

The Australian Constitution does not expressly protect freedom of expression.

However, the High Court has found, in a series of cases beginning in 1992,\(^{43}\) that the Constitution implies a freedom of political communication, which protects the freedom to communicate on governmental or political matters—although the precise scope of the communications protected is uncertain.

The questions to be determined in identifying whether the implied freedom of political communication will invalidate a law in any given case were explained by the High Court in *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520 and refined in *Coleman v Power* (2004) 220 CLR 1 and very recently in *McCloy v State of New South Wales* [2015] HCA 34 (7 October 2015), per French CJ, Kiefel, Bell and Keane JJ at [2]-[5]. In summary form, they are as follows:

1. Does the law effectively burden freedom of communication about government or political matters in its terms, operation or effect?
   
   If ‘no’, then the law does not exceed the implied limitation and the enquiry as to validity ends.

2. If ‘yes’ to question 1, are the purpose of the law and the means adopted to achieve that purpose legitimate, in the sense that they are compatible with the maintenance of the constitutionally prescribed system of representative and responsible government?
   
   The answer to that question will be in the affirmative if the purpose of the law and the means adopted do not adversely impinge on the functioning of the system of representative government.

3. If ‘yes’ to question 2, is the law reasonably appropriate and adapted to advance that legitimate object?
   
   This involves a proportionality test, which involves considering the extent of the burden effected by the impugned provision on the freedom. There are three stages to the test—these are the enquiries as to whether the law is justified as suitable, necessary and adequate in its balance in the following senses:

---

Suitable—as having a rational connection to the purpose of the provision.

Necessary—in the sense that there is no obvious and compelling alternative reasonably practicable means of achieving the same purpose, which has a less restrictive effect on the freedom.

Adequate in its balance—a criterion requiring a value judgment, consistently with the limits of the judicial function, describing the balance between the importance of the purpose served by the restrictive measure and the extent of the restriction it imposes on the freedom.

In this context, the same judges made the following significant comment (at [84]):

It is not possible to ignore the importance of a legislative purpose in considering the reasonableness of a legislative measure because that purpose may be the most important factor in justifying the effect that the measure has on the freedom. The submissions for the Commonwealth bear this out. The Commonwealth submitted that the Court cannot consider the relationship between the means adopted by the law and ‘the constitutional imperative’ to not infringe the freedom without having the object of the law in view, for some statutory objects may justify very large incursions on the freedom. The example the Commonwealth gave was the object of protecting security of a nation at a time of war.

Application of the implied freedom in relation to secrecy laws

A Commonwealth public service regulation which provided that relevant officials had a duty (in effect) to maintain the secrecy of all official information, regardless of whether it might cause harm to the public interest (in circumstances where section 70 of the Crimes Act creates an offence relating to a disclosure made in breach of such a duty) was found to infringe the implied constitutional freedom of political communication in the Bennett case44.

The case involved a public servant (Bennett) who made certain public comments after having been formally directed by the CEO of Customs (a public service agency) to refrain from doing so. Bennett was disciplined for breach of regulation 7(13) of the Public Service Regulations 1999 and his complaint to the Human Rights and Equal Opportunity Commission was unsuccessful. Bennett sought judicial review in the Federal Court, arguing that regulation 7(13) was invalid as it infringed the implied freedom of political communication.

Regulation 7(13) provided as follows:

An APS employee must not, except in the course of his or her duties as an APS employee or with the Agency Head’s express authority, give or disclose, directly or indirectly, any information about public business or anything of which the employee has official knowledge.

The Federal Court (Finn J) held the regulation to be invalid. The Court relevantly commented as follows.

Official secrecy has a necessary and proper province in our system of government. A surfeit of secrecy does not. It is unnecessary to enlarge upon why I consider the regulation to be an inefficient provision other than to comment that its ambit is such that even the most scrupulous public servant would find it imposes ‘an almost impossible demand’ in domestic, social and work related settings …

The dimensions of the control it imposes impedes quite unreasonably the possible flow of information to the community—information which, without possibly prejudicing the interests of the Commonwealth, could only serve to enlarge the public’s knowledge and understanding of the operation, practices and policies of executive government.

Regulation 7(13) was subsequently replaced by regulation 2.1, which was later unsuccessfully challenged in the Supreme Court of the ACT on the same constitutional basis. Regulation 2.1 relevantly provided for the scope of the relevant duty as follows:

2.1 **Duty not to disclose information (Act s 13)**

1. This regulation is made for subsection 13(13) of the Act.

2. This regulation does not affect other restrictions on the disclosure of information.

3. An APS employee must not disclose information which the APS employee obtains or generates in connection with the APS employee’s employment if it is reasonably foreseeable that the disclosure could be prejudicial to the effective working of government, including the formulation or implementation of policies or programs.

---

(4) An APS employee must not disclose information which the APS employee obtains or generates in connection with the APS employee’s employment if the information:

(a) was, or is to be, communicated in confidence within the government; or

(b) was received in confidence by the government from a person or persons outside the government;

whether or not the disclosure would found an action for breach of confidence.

While section 35P is cast in broad terms, the information to which it applies must at least ‘relate to’ an SIO, which is an operational ASIO activity. As far as ASIO officials and other ‘insiders’ are concerned, the information caught by section 35P is effectively a subset of the information caught by section 18 of the ASIO Act. Any constitutional concern in relation to the implied freedom would apply with greater force in relation to section 18 than to section 35P, as the former is not linked to operational information.46

This report is concerned with the question of the impact on outsiders—third parties such as journalists. National security including counter-terrorism and ASIO’s conduct are of legitimate concern in relation to government and politics. Section 35P burdens discussion about such matters.

The next question is whether the purpose of section 35P and the means adopted to achieve that purpose are compatible with maintaining the constitutionally prescribed system of representative and responsible government. The answer to that question would likely be ‘yes’, on the basis that the purpose of section 35P (broadly) is to protect national security.

The last question is whether section 35P is reasonably appropriate and adapted to serve that legitimate end, applying the proportionality test. Criticisms of section 35P, reflected in this report include: the width of the information caught; the application to information of no operational relevance; the prohibition being unlimited in time and space; the absence in the basic offence of an express harm requirement; the difficulty if not impossibility of knowing what is prohibited and the application of the prohibition to information already in the public domain. These criticisms combine to give substance to an argument that the answer to the

46 See the comments of Dr AJ Brown concerning the constitutional test of proportionality in this context, specifically, in connection with the PID Act regime, referred to in Appendix I.
last question is ‘no’. On that basis, section 35P would be invalid. It is difficult to see how this section might be read down, unless it was limited to ASIO employees and ASIO affiliates. In this regard, it is worth noting, as discussed earlier in the report, that applying the ordinary meaning of the word ‘disclose’ rather than the wide meaning contended by the authorities would arguably not catch publication by a journalist who does not have actual knowledge of the information disclosed.

International law

Australia is a party to the International Covenant on Civil and Political Rights (ICCPR). Article 19 of the ICCPR provides as follows:

Article 19

1. Everyone shall have the right to hold opinions without interference.

2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided for by law and are necessary:

   (a) For respect of the rights or reputations of others;

   (b) For the protection of national security or of public order (ordre public), or of public health or morals.

While there may be various international human rights laws of relevance, article 19 of the ICCPR appears to be the most obviously relevant and was the main focus of attention in submissions to the inquiry and in the parliamentary processes (including review by the PJCIS and the Parliamentary Joint Committee on Human Rights) associated with the NSLAB (No 1) 2014 (see Appendix B). Principles of treaty

---

47 See Monis v The Queen (2013) 249 CLR 92, in which differing views were expressed by members of the High Court as to the extent to which it was permissible to read down a provision to identify the purpose of the provision, which is critical to determining whether the provision may infringe the implied freedom.

interpretation are set out in the *Vienna Convention on the Law of Treaties* [1974] ATS 2, in force generally and for Australia, 27 January 1980.\(^{49}\)

Provisions of a treaty to which Australia is a party do not form part of Australian law unless those provisions have been incorporated by statute.\(^{50}\) Treaties may have an indirect effect on the interpretation of domestic law\(^{51}\) and as a source of development of the common law (the decision of the High Court in *Mabo v Queensland (No 2)* (1992) 175 CLR 1 providing a well-known example). Australia may also be the subject of complaints to the United Nations Human Rights Committee.\(^{52}\)

Section 8 of the INSLM Act obliges the INSLM to have regard to Australia’s obligations under international instruments. Those instruments are not limited to those enacted as part of domestic law. Several submissions to this inquiry, including the Australian Human Rights Commission submission, also referred to the *Tshwane Principles*\(^{53}\) as providing relevant guidance on issues relating to national security and the right to government information. Those Principles are not international obligations in the sense used in section 8 of the INSLM Act.

The following are selected extracts from General Comment No 34 of the United Nations Human Rights Committee, Article 19, *Freedoms of opinion and expression* (2011) UN Doc CCPR/C/GC/34, 12 September 2011 (footnotes omitted). The views of the United Nations Human Rights Committee are not binding, but are persuasive. This lengthy extract is included because it goes to the heart of the issues involved in this inquiry and provides a considered international context:

49 See articles 31 and 32 in particular.
52 In this regard, Australia is a party to the *First Optional Protocol to the International Covenant on Civil and Political Rights* [1991] ATS 39, in force generally 23 March 1976 and for Australia, 25 December 1991.
General Comment No 34

Article 19: Freedoms of opinion and expression

General remarks

2. Freedom of opinion and freedom of expression are indispensable conditions for the full development of the person. They are essential for any society. They constitute the foundation stone for every free and democratic society. The two freedoms are closely related, with freedom of expression providing the vehicle for the exchange and development of opinions.

3. Freedom of expression is a necessary condition for the realization of the principles of transparency and accountability that are, in turn, essential for the promotion and protection of human rights.

7. The obligation to respect freedoms of opinion and expression is binding on every State party as a whole. All branches of the State (executive, legislative and judicial) and other public or governmental authorities, at whatever level – national, regional or local – are in a position to engage the responsibility of the State party. Such responsibility may also be incurred by a State party under some circumstances in respect of acts of semi-State entities...

Freedom of expression

11. Paragraph 2 requires States parties to guarantee the right to freedom of expression, including the right to seek, receive and impart information and ideas of all kinds regardless of frontiers. This right includes the expression and receipt of communications of every form of idea and opinion capable of transmission to others, subject to the provisions in article 19, paragraph 3, and article 20. It includes political discourse, commentary on one’s own and on public affairs, canvassing, discussion of human rights, journalism, cultural and artistic expression, teaching, and religious discourse. It may also include commercial advertising. The scope of paragraph 2 embraces even expression that may be regarded as deeply offensive, although such expression may be restricted in accordance with the provisions of article 19, paragraph 3 and article 20.

12. Paragraph 2 protects all forms of expression and the means of their dissemination. Such forms include spoken, written and sign language and such non-verbal expression as images and objects of art. Means of expression include books, newspapers, pamphlets, posters, banners, dress and legal
submissions. They include all forms of audio-visual as well as electronic and internet-based modes of expression.

**Freedom of expression and the media**

13. A free, uncensored and unhindered press or other media is essential in any society to ensure freedom of opinion and expression and the enjoyment of other Covenant rights. It constitutes one of the cornerstones of a democratic society. The Covenant embraces a right whereby the media may receive information on the basis of which it can carry out its function. The free communication of information and ideas about public and political issues between citizens, candidates and elected representatives is essential. This implies a free press and other media able to comment on public issues without censorship or restraint and to inform public opinion. The public also has a corresponding right to receive media output.

... 

15. States parties should take account of the extent to which developments in information and communication technologies, such as internet and mobile based electronic information dissemination systems, have substantially changed communication practices around the world. There is now a global network for exchanging ideas and opinions that does not necessarily rely on the traditional mass media intermediaries. States parties should take all necessary steps to foster the independence of these new media and to ensure access of individuals thereto.

... 

**Right of access to information**

18. Article 19, paragraph 2 embraces a right of access to information held by public bodies. Such information includes records held by a public body, regardless of the form in which the information is stored, its source and the date of production. Public bodies are as indicated in paragraph 7 of this general comment. The designation of such bodies may also include other entities when such entities are carrying out public functions. As has already been noted, taken together with article 25 of the Covenant, the right of access to information includes a right whereby the media has access to information on public affairs and the right of the general public to receive media output. Elements of the right of access to information are also addressed elsewhere in the Covenant...

19. To give effect to the right of access to information, States parties should proactively put in the public domain Government information of public interest. States parties should make every effort to ensure easy, prompt,
effective and practical access to such information. States parties should also enact the necessary procedures, whereby one may gain access to information, such as by means of freedom of information legislation...

...  

**The application of article 19(3)**  

21. Paragraph 3 expressly states that the exercise of the right to freedom of expression carries with it special duties and responsibilities. For this reason two limitative areas of restrictions on the right are permitted, which may relate either to respect of the rights or reputations of others or to the protection of national security or of public order (*ordre public*) or of public health or morals. However, when a State party imposes restrictions on the exercise of freedom of expression, these may not put in jeopardy the right itself...

22. Paragraph 3 lays down specific conditions and it is only subject to these conditions that restrictions may be imposed: the restrictions must be “provided by law”; they may only be imposed for one of the grounds set out in subparagraphs (a) and (b) of paragraph 3; and they must conform to the strict tests of necessity and proportionality. Restrictions are not allowed on grounds not specified in paragraph 3, even if such grounds would justify restrictions to other rights protected in the Covenant. Restrictions must be applied only for those purposes for which they were prescribed and must be directly related to the specific need on which they are predicated.

23. States parties should put in place effective measures to protect against attacks aimed at silencing those exercising their right to freedom of expression...

24. Restrictions must be provided by law. Law may include laws of parliamentary privilege...

25. For the purposes of paragraph 3, a norm, to be characterized as a “law”, must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public. A law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution. Laws must provide sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not.

26. Laws restricting the rights enumerated in article 19, paragraph 2, including the laws referred to in paragraph 24, must not only comply with the strict requirements of article 19, paragraph 3 of the Covenant but must also
themselves be compatible with the provisions, aims and objectives of the Covenant...

27. It is for the State party to demonstrate the legal basis for any restrictions imposed on freedom of expression. If, with regard to a particular State party, the Committee has to consider whether a particular restriction is imposed by law, the State party should provide details of the law and of actions that fall within the scope of the law.

28. The first of the legitimate grounds for restriction listed in paragraph 3 is that of respect for the rights or reputations of others.

29. The second legitimate ground is that of protection of national security or of public order (ordre public), or of public health or morals.

30. Extreme care must be taken by States parties to ensure that treason laws and similar provisions relating to national security, whether described as official secrets or sedition laws or otherwise, are crafted and applied in a manner that conforms to the strict requirements of paragraph 3. It is not compatible with paragraph 3, for instance, to invoke such laws to suppress or withhold from the public information of legitimate public interest that does not harm national security or to prosecute journalists, researchers, environmental activists, human rights defenders, or others, for having disseminated such information...

33. Restrictions must be “necessary” for a legitimate purpose. Thus, for instance, a prohibition on commercial advertising in one language, with a view to protecting the language of a particular community, violates the test of necessity if the protection could be achieved in other ways that do not restrict freedom of expression...

34. Restrictions must not be overbroad. The Committee observed in general comment No. 27 that “restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve their protective function; they must be proportionate to the interest to be protected...The principle of proportionality has to be respected not only in the law that frames the restrictions but also by the administrative and judicial authorities in applying the law”. The principle of proportionality must also take account of the form of expression at issue as well as the means of its dissemination. For instance, the value placed by the Covenant upon uninhibited expression is particularly high in the circumstances of public
debate in a democratic society concerning figures in the public and political domain.

35. When a State party invokes a legitimate ground for restriction of freedom of expression, it must demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat.

...  

38. As noted earlier in paragraphs 13 and 20, concerning the content of political discourse, the Committee has observed that in circumstances of public debate concerning public figures in the political domain and public institutions, the value placed by the Covenant upon uninhibited expression is particularly high...

42. The penalization of a media outlet, publishers or journalist solely for being critical of the government or the political social system espoused by the government can never be considered to be a necessary restriction of freedom of expression.

43. Any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government.

44. Journalism is a function shared by a wide range of actors, including professional full-time reporters and analysts, as well as bloggers and others who engage in forms of self-publication in print, on the internet or elsewhere, and general State systems of registration or licensing of journalists are incompatible with paragraph 3. Limited accreditation schemes are permissible only where necessary to provide journalists with privileged access to certain places and/or events. Such schemes should be applied in a manner that is non-discriminatory and compatible with article 19 and other provisions of the Covenant, based on objective criteria and taking into account that journalism is a function shared by a wide range of actors.
45. It is normally incompatible with paragraph 3 to restrict the freedom of journalists and others who seek to exercise their freedom of expression (such as persons who wish to travel to human rights-related meetings) to travel outside the State party, to restrict the entry into the State party of foreign journalists to those from specified countries or to restrict freedom of movement of journalists and human rights investigators within the State party (including to conflict-affected locations, the sites of natural disasters and locations where there are allegations of human rights abuses). States parties should recognize and respect that element of the right of freedom of expression that embraces the limited journalistic privilege not to disclose information sources.

46. States parties should ensure that counter-terrorism measures are compatible with paragraph 3. Such offences as “encouragement of terrorism” and “extremist activity” as well as offences of “praising”, “glorifying”, or “justifying” terrorism, should be clearly defined to ensure that they do not lead to unnecessary or disproportionate interference with freedom of expression. Excessive restrictions on access to information must also be avoided. The media plays a crucial role in informing the public about acts of terrorism and its capacity to operate should not be unduly restricted. In this regard, journalists should not be penalized for carrying out their legitimate activities.

The main question for purpose of this inquiry is whether the restrictions on freedom of expression imposed by section 35P are ‘necessary’ for the protection of national security.

This issue involves applying a ‘proportionality’ test—that is, broadly, that the law is appropriate and involves the least restrictive means needed to achieve its protective function.\(^{54}\)

\(^{54}\) See paragraph 34 of General Comment No 34 of the UN Human Rights Committee (extracted below). The Explanatory Memorandum to the NSLA Bill (No 1) 2014 and other official documents provided to the Parliament or to this inquiry in relation to section 35P seemingly refer to the same broad test.
Differing views have been expressed about whether section 35P meets the proportionality test:

- The Government maintains that it does. See for example:
  - the relevant extract from the Explanatory Memorandum to the NSLAB (No 1) 2014 and other comments from the Government also included in Appendix B, and
  - Attachment A to Submission 24 to this inquiry (from AGD, in response to requests for information).
- The Senate Standing Committee for the Scrutiny of Bills made comments (not directly linked to article 19 of the ICCPR and also set out in Appendix B) indicating a concern that the offences could perhaps be more directly connected and proportionate to the achievement of the relevant protective purposes.
- The Parliamentary Joint Committee on Human Rights considered the new offence provisions for disclosing information regarding SIOs to be incompatible with the right to freedom of expression because they appeared to impose disproportionate limits on that right.
- Many submissions to this inquiry stated that section 35P (especially the basic offence) was disproportionate to the protective purposes of the provision.

None of the submissions received by this inquiry made reference to any Australian jurisprudence directly dealing with the question of consistency with article 19 of the ICCPR.

The issues in connection with article 19 are not unlike those in connection with constitutional validity as far as the implied freedom of political communication is concerned. A conclusion that section 35P is inconsistent with article 19 of the ICCPR is more likely than a conclusion that section 35P infringes the implied freedom of political communication. This is because necessity (and proportionality) is directly in issue, rather than being seen through the prism of the implied freedom of political communication. Recognising that opinions can and do vary on this issue, the argument that section 35P is inconsistent with article 19 is persuasive.
A related United Kingdom case

A related issue in a national security context in the United Kingdom was dealt with by the House of Lords in *R v Shayler* [2003] 1 AC 247. The *Shayler* case concerned the relevant question whether certain provisions including section 1(1) of the *Official Secrets Act 1989* (UK) which created secrecy offences directed at intelligence community ‘insiders’ were compatible with article 10 of the *European Convention on Human Rights* (ECHR, a provision broadly akin to article 19 of the ICCPR). Shayler was a former member of the British security service who disclosed publicly (through the media) various classified and sensitive matters of which he had knowledge by virtue of that former position. He argued that the disclosures were made in the public interest and, as such, were protected.

The House of Lords held that the provisions were consistent with article 10 of the ECHR. In this regard, the House of Lords considered it was significant that there were various avenues for making permitted disclosures and a capacity for disclosures to be authorised. Article 10 of the ECHR is not identical to article 19 of the ICCPR so the *Shayler* case is not directly relevant as a legal matter for present purposes, but it offers an insight into related issues.

The United Kingdom is also a party to the ICCPR. According to the Australian Law Reform Commission (ALRC) (footnote omitted):

> 8.49 Section 1(1) of the *Official Secrets Act* has also been considered by the United Nations Human Rights Committee. While the Committee did not state that the provision itself was incompatible with art 19 of the ICCPR, it expressed concern about the way in which the provision was enforced. It noted that disclosures of information may be penalised under the *Official Secrets Act 1989* even where they are not harmful to national security, and that powers under the Act have been ‘exercised to frustrate former employees of the Crown from bringing into the public domain issues of genuine public concern’.

The Committee observed that:

> The State party must ensure that its powers to protect information genuinely related to matters of national security are narrowly utilized and limited to instances where the release of such information would be harmful to national security.
Appendix K—The controlled operations precedent for the SIO scheme and section 35P

History of the controlled operations scheme

The SIO scheme in Division 4 of Part III of the ASIO Act is modelled on the controlled operations scheme in Part IAB of the Crimes Act.

It is instructive to consider the history and purpose of the controlled operations scheme on which the SIO scheme is based.

Key aspects of the legislative history of the controlled operations scheme are:

- the scheme was introduced by the *Crimes Amendment (Controlled Operations) Act 1996* (No 28 of 1996) in response to the decision of the High Court in *Ridgeway v R* (1995) 184 CLR 19 and was initially limited to operations connected with the narcotic drug offences
- the scheme was amended by the *Measures to Combat Serious and Organised Crime Act 2001* (No 136 of 2001) to expand the operation of the scheme to apply to the investigation of a much wider range of serious Commonwealth offences and to expand the exemption from criminal liability to cover Commonwealth, State and Territory offences, and
- the scheme was amended by the *Crimes Legislation Amendment (Serious and Organised Crime) Act 2010* (No 3 of 2010) which implemented national model laws for controlled operations as part of a national response to organised crime (including sections 15HK and 15HL, on which section 35P of the ASIO Act was modelled).

The following extract relating to the controlled operations scheme is from a February 2003 Discussion Paper entitled *Cross-border Investigative Powers for Law Enforcement* prepared by a Joint Working Group for the Standing Committee of Attorneys-General and Australasian Police Ministers Council Joint Working Group on National Investigation Powers (footnotes omitted):

**What is a controlled operation?**

A ‘controlled operation’ is an investigative method used by law enforcement agencies to identify suspects, obtain evidence and allow suspects to be prosecuted. It may be used to investigate a range of criminal offences such as murder, money laundering, forms of trafficking, smuggling, corruption and bribery. The aim of a
controlled operation is often to gather evidence and intelligence against those who organise and finance crime, rather than merely focussing on couriers and intermediaries.

In a controlled operation, instead of seeking to terminate immediately a criminal scheme, law enforcement officers allow the scheme to unfold under controlled conditions. During the process of allowing the scheme to unfold, an informant, agent or undercover police officer may themselves need to commit offences (for example, they may need to possess or sell an illicit drug).

Although controlled operations have been used in law enforcement for many years, there was no legislation that comprehensively regulated their use in Australia until 1995. Up until that time, police operatives who became involved in criminal activities as part of an operation were in many circumstances liable to be charged with criminal offences, but relied on other police and prosecutors to refrain from charging and prosecuting them with offences arising from their work. When making this decision, the police or prosecutor ordinarily takes into account all of the circumstances surrounding the offences and weighs up the public interest in pursuing a prosecution.

Law enforcement agencies also relied on persuading the courts to allow the evidence gathered during the operation to be used in the trial against the accused person. However, this approach changed in 1995 following the High Court decision in Ridgeway v The Queen.

Ridgeway was arrested by the Australian Federal Police (AFP) with 203 grams of heroin in his possession and convicted in the South Australian District Court for possessing a prohibited import (heroin). The prosecution alleged that Ridgeway initiated a deal to import heroin into Australia and to purchase the drug when it arrived. The importation of the drug had been undertaken by a police informer with the assistance of the AFP and the Malaysian Police in a ‘controlled delivery’ arranged for the purpose of apprehending Ridgeway. Ridgeway appealed his conviction to the High Court of Australia, which allowed his appeal and granted a permanent stay of proceedings in his favour.

The High Court decided that the importation of the heroin by law enforcement officers was illegal and therefore the evidence of that importation should have been excluded from the trial on the grounds of public policy.

The Court explained that judges may decide to exclude evidence obtained during an illegal activity involving law enforcement officers. In deciding, the Court weighs up the public interest in discouraging unlawful conduct by law enforcement officers against the public interest in the conviction of wrongdoers. In this case, the Court took into account the nature and the degree of the law enforcement officers’
unlawful conduct and the fact that the unlawful importation of the drug by the police created an element of the offence charged against Ridgeway (possession of a prohibited import). The Court was also concerned that there was no official disapproval of the criminal activity undertaken by the officers.

In the particular circumstances of Ridgeway’s case, the Court decided that the public interest was better served by excluding the evidence obtained through the illegal importation of the heroin. The Court acknowledged that sometimes law enforcement officers need to engage in a range of activities, in some cases illegal, to uncover organised crime, and recommended that the problems relating to the conduct of controlled operations should be addressed by introducing regulating legislation.

The response to the Ridgeway decision

As a result of the Ridgeway decision, a number of Australian jurisdictions (South Australia in 1995, the Commonwealth in 1996, New South Wales in 1997, and Queensland in 2000) enacted legislation providing for controlled operations. These provisions set out a process for authorising illegal activities by law enforcement agencies.

Controlled operations—why legislate?

Controlled operations legislation has been in place in Australian jurisdictions for a number of years and the issues surrounding its use have been articulated and debated in government and parliamentary reviews, as well as royal commissions. These reviews, while recognising the dangers of authorising illegal activities, have concluded that a legislative approach is the best way of limiting and monitoring such law enforcement activity.

For example, the Wood Royal Commission into the NSW Police Service considered the use of covert operations in the Police Service and recommended the introduction of regulating legislation because it would introduce greater regularity and certainty into undercover operations and resolve concerns about the criminal and civil liability of officers and civilians assisting them.

Also, a major review of the Commonwealth controlled operations legislation was undertaken by the Parliamentary Joint Committee (PJC) on the National Crime Authority (NCA) in 1999.

At that time, the Commonwealth legislation authorising controlled operations applied only in relation to the investigation of offences involving the importation of narcotics. One of the tasks of the PJC inquiry was to consider whether the
Commonwealth controlled operations provisions ought be extended to a greater range of Commonwealth offences. The PJC’s report, *Street Legal*, discusses the key issues in relation to controlled operations including the desirability of regulating such operations by legislation.

The PJC noted the advantages of a legislative approach in that it:

- provides clear guidance as to what are acceptable and unacceptable activities; (This ensures that the public interest in convicting wrong doers is balanced against the need to ensure that those entrusted with law enforcement do not impeach the integrity of the system.)
- provides protection for covert police officers so they can perform their duties in the knowledge that they will not be prosecuted for undertaking necessary, authorised activities;
- lessens the risk that evidence might be judicially excluded;
- imposes internal discipline on law enforcement agencies; and
- provides a scheme of accountability that can be monitored and reviewed, and which makes the behaviour of law enforcement officers subject to independent scrutiny.

The PJC also identified possible disadvantages of controlled operations legislation in that it:

- legalises crimes committed by law enforcement officers;
- might lead to the commission of offences which, but for the activities of the law enforcement officers, might not have been committed; and
- may be susceptible to “function creep”. In other words, the legislation may be introduced for a limited purpose with a particular justification. Over time it might then be progressively extended to cover a wider range of purposes without sufficient additional justification.

The PJC concluded that while this type of legislation does have disadvantages, controlled operations are a necessary tool in law enforcement providing that proper checks and balances to ensure that the rights of citizens and the judicial system were not undermined. The PJC recommended that the Commonwealth, States and Territories work together to harmonise controlled operations regimes across Australia.
Background to the controlled operations precedent

Discussion paper: Cross-border Investigative Powers for Law Enforcement

The Discussion Paper Cross-border Investigative Powers for Law Enforcement (referred to above) included a proposed clause 27 dealing with unauthorised disclosure of information, as follows:

Unauthorised disclosure of information

(1) A person who discloses any information relating to a cross-border controlled operation or a corresponding authorised operation is guilty of an offence unless the disclosure is made:
(a) In connection with the administration or execution of [these Model Provisions] or a corresponding law, or
(b) For the purposes of any legal proceeding arising out of or otherwise related to [these Model Provisions] or a corresponding law or of any report of any such proceedings, or
(c) In accordance with any requirement imposed by law.

Maximum penalty: Imprisonment for 2 years.

(2) A person is guilty of an offence against this subsection if the person commits an offence against subsection (1) in circumstances in which the person is reckless as to whether the disclosure of information endangers the health or safety of any person or prejudices the effective conduct of a cross-border controlled operation.

Maximum penalty: Imprisonment for 10 years.

The Discussion Paper included the following brief reasoning in relation to this clause:

To protect persons participating in controlled operations and to ensure the integrity of investigations, it will be an offence for a person to intentionally disclose information about a cross-border controlled operation, whether it is authorised in the local jurisdiction or elsewhere.

A penalty of up to 10 years imprisonment will apply where the person is reckless as to whether the disclosure endangers the health and safety of a person or prejudices the effective conduct of an operation. A penalty of up to two years imprisonment would apply to other disclosures.
Report: Cross-border Investigative Powers for Law Enforcement
The Discussion Paper was followed by the November 2003 report entitled Cross-border Investigative Powers for Law Enforcement, also prepared by a Joint Working Group for the Standing Committee of Attorneys-General and Australasian Police Ministers Council Joint Working Group on National Investigation Powers. That report included a proposed clause 22 (Unauthorised disclosure of information), as follows:

Unauthorised disclosure of information

(1) A person is guilty of an offence if:
   (a) the person intentionally, knowingly or recklessly discloses any information; and
   (b) the person knows that, or is reckless as to whether, the information relates to an authorised operation or a corresponding authorised operation; and
   (c) the person knows that, or is reckless as to whether, the disclosure is not made:
      (i) in connection with the administration or execution of [these model provisions] or a corresponding law; or
      (ii) for the purposes of any legal proceeding arising out of or otherwise related to [these model provisions] or a corresponding law or of any report of any such proceedings; or
      (iii) in accordance with any requirement imposed by law.

Penalty: Imprisonment for 2 years.

(2) A person is guilty of an offence against this sub-section if the person commits an offence against sub-section (1) in circumstances in which the person:
   (a) intends to endanger the health or safety of any person or prejudice the effective conduct of an authorised operation or a corresponding authorised operation; or
   (b) knows that, or is reckless as to whether, the disclosure of the information:
      (i) endangers or will endanger the health or safety of any person; or
      (ii) prejudices or will prejudice the effective conduct of an authorised operation or a corresponding authorised operation.

Penalty: Imprisonment for 10 years.
This 2003 report included the following discussion in relation to proposed clause 27 from the Discussion Paper (footnotes omitted, and the reference to the ‘CBA’ is to the Criminal Bar Association-Victoria):

Submissions and responses

The CBA opposed the provision as drafted in the Discussion Paper arguing that given the seriousness of the maximum penalties for these offences, the provision should take account of the knowledge, intention and recklessness of the person who discloses the information relating to an authorised controlled operation. This argument was supported by the Victorian Bar and the Law Council of Australia. The NSWCCL, the ICJ-AS and Privacy New South Wales made similar arguments.

Conclusion

The JWG intends that all of the offences created by the model bills will require a subjective fault element. Currently, different jurisdictions have different approaches to fault elements when none are expressed in the offence. To ensure that the offences operate consistently in all participating jurisdictions, an express fault element has been included for each physical element of the offences.

A person will not be guilty of an offence under these provisions unless he or she intentionally, knowingly or recklessly discloses information relating to an authorised operation.

To commit the offence under clause 22(1), which carries a penalty of up to 2 years imprisonment, a person would need to:

- Intentionally, knowingly or recklessly disclose information;
- Know that, or be reckless as to whether, the information is about a cross-border controlled operation; and
- Know that, or be reckless as to whether, he or she is not authorised to disclose the information.

To commit the offence under clause 22(2), which carries a penalty of up to 10 years imprisonment, a person would need to do those things set out above, and:

- Intend, know or be reckless as to whether, a person or investigation is endangered by disclosing the information.
Crimes Legislation Amendment (Serious and Organised Crime) Bill 2010

The Explanatory Memorandum to the Crimes Legislation Amendment (Serious and Organised Crime) Bill 2010 contains the following explanation relating to Schedule 3 to that Bill:

In April 2009, the Standing Committee of Attorneys-General (SCAG) agreed to a set of resolutions for a comprehensive national response to combat organised crime. The SCAG resolutions dealt with both the legislative and operational response to organised criminal activity. This Bill implements the Commonwealth’s commitment as part of the SCAG agreement to enhance its legislation to combat organised crime by:

- enhancing police powers to investigate organised crime by implementing model laws for controlled operations, assumed identities and witness identity protection (Schedule 3)

Schedule 3 will replace the existing provisions in the Crimes Act 1914 for controlled operations, assumed identities and witness identity protection with the model laws, taking into account the unique role of Commonwealth agencies for national security and the investigation of crimes with a foreign aspect.

The purpose of this Schedule is to replace the existing controlled operations, assumed identities and witness identity protection regimes in the Crimes Act 1914 with new regimes based on national model legislation. The laws were developed following the 2002 Leaders Summit on Multi-jurisdictional Crime by the Joint Working Group of the Standing Committee of Attorneys-General (SCAG) and the then Australasian Police Ministers Council. The Joint Working Group Report, Cross-border Investigative Powers for Law Enforcement, was released in November 2003, and the model laws endorsed for implementation by SCAG in 2004.

The intent of the model legislation is to harmonise, as closely as possible, the controlled operations, assumed identities and protection of witness identity regimes across Australia and enable authorisations issued under a regime in one jurisdiction to be recognised in other jurisdictions.

The model laws are intended to enhance the ability of law enforcement agencies to investigate and prosecute multi-jurisdictional criminal activity. This type of crime is becoming increasingly common due to advances in information and communication technology, and the increasing sophistication of organised criminal groups,
particularly those involved in terrorism or trans-national crime, including drug trafficking. State and Territory adoption of the model laws will:

- allow an authority for a cross-border controlled operation issued in one jurisdiction to be recognised in other participating jurisdictions, which will permit the movement of State or Territory controlled operatives across the State or Territory border without the need to make a separate application for a controlled operation in the second jurisdiction
- enable a person authorised to acquire and use an assumed identity in one jurisdiction to lawfully acquire evidence of that assumed identity in another jurisdiction, and
- enable a witness identity protection certificate that is issued in one jurisdiction to be recognised in proceedings held in another jurisdiction, which will protect the identity of operatives as they move across State or Territory borders without the need to seek separate certificates.

**Crimes Act**

Section 15HK and 15HL of the Crimes Act as amended provided (and still provide, but with additional exceptions in respect of an integrity testing controlled operation authority, and misconduct, respectively) as follows:

**Section 15HK**

**Unauthorised disclosure of information**

(1) A person is guilty of an offence if:

(a) the person discloses information; and

(b) the information relates to a controlled operation.

Penalty: Imprisonment for 2 years.

Exceptions-general

(2) Subsection (1) does not apply if the disclosure was:

(a) in connection with the administration or execution of this Part; or

(b) for the purposes of any legal proceedings arising out of or otherwise related to this Part or of any report of any such proceedings; or

(c) for the purposes of obtaining legal advice in relation to the controlled operation; or

(d) in accordance with any requirement imposed by law; or

(e) in connection with the performance of functions or duties, or the exercise of powers, of a law enforcement agency.

Note: A defendant bears an evidential burden in relation to the matters in this subsection-see subsection 13.3(3) of the *Criminal Code*. 
Section 15HL

Unauthorised disclosure of information-endangering safety, etc.

(1) A person is guilty of an offence if-
   (a) the person discloses information; and
   (b) the information relates to a controlled operation; and
   (c) either:
       (i) the person intends to endanger the health or safety of any person or prejudice the effective conduct of a controlled operation; or
       (ii) the disclosure of the information will endanger the health or safety of any person or prejudice the effective conduct of a controlled operation.

Penalty: Imprisonment for 10 years.

Exceptions-general

(3) Subsection (1) does not apply if the disclosure was:
   (a) in connection with the administration or execution of this Part; or
   (b) for the purposes of any legal proceedings arising out of or otherwise related to this Part or of any report of any such proceedings; or
   (c) for the purposes of obtaining legal advice in relation to the controlled operation; or
   (d) in accordance with any requirement imposed by law; or
   (e) in connection with the performance of functions or duties, or the exercise of powers, of a law enforcement agency.

Note: A defendant bears an evidential burden in relation to the matters in this subsection—see subsection 13.3(3) of the Criminal Code.

Fault elements

The main change to the model unauthorised disclosure provisions in the Discussion Paper (proposed clause 27) that were made in the Report of the Joint Working Group (proposed clause 22) appears to be the change to the relevant fault elements.

Proposed clause 27 did not contain an express fault element in respect of the disclosure of information relating to a controlled operation, whereas proposed clause 22 applied where a person made a relevant disclosure intentionally, knowingly or recklessly. Clause 22 further provided that the person need only know that, or be reckless as to whether, the information related to a controlled operation. Section 15HK and 15HL (and section 35P of the ASIO Act) do not use the
words ‘intentionally’, ‘knowingly’ or ‘recklessly’ in relation to disclosing information that relates to a relevant operation.

(The offences under sections 15HK and 15HL of the Crimes Act and under section 35P of the ASIO Act involve disclosing information that relates to a relevant operation. No fault element is expressly provided in relation to the circumstance that the disclosure relates to a relevant operation. Therefore, the effect of the Criminal Code is that recklessness is the fault element in this respect.)

Likewise, in relation to the aggravated offence, proposed clause 27 contained only the fault element of recklessness in connection with the harm which might ensue from an unauthorised disclosure, whereas proposed clause 22 referred expressly to intention and knowledge as well as recklessness in this context. The concern in this respect appears to have been that a 10-year penalty for a disclosure made recklessly in this respect might not be appropriate, and that the offence should also refer to a person’s intention or knowledge in relation to harm, so that gradations of culpability are expressly recognised.

The extract from the Explanatory Memorandum set out above states that the new controlled operations regime was ‘based on’ the model national legislation. As is apparent from the summary above, there were some differences between sections 15HK and 15HL and the model laws. Section 15HL (the aggravated offence, like section 35P(2)) does, however, reflect gradations of culpability.

**Initial disclosure and re-publication**
There is no discussion in this history about whether the prohibition on disclosure was intended to apply to persons other than police officers and others involved in or having actual knowledge of controlled operations. In particular, there is no justification or explanation for not distinguishing between initial disclosure and re-publication, if that were intended. This omission is striking in view of the fact that secrecy provisions were the subject of active consideration by the Australian Law Reform Commission (ALRC) and interested parties during 2008–09 (leading to ALRC Report No 112, Secrecy Laws and Open Government in Australia, December 2009). The Senate Legal and Constitutional Affairs Committee reported in September 2009 on the Crimes Legislation Amendment (Serious and Organised Crime) Bill 2009, without discussing the secrecy offences relating to controlled operations in any detail. The same applies in relation to an earlier version of the Bill, the Crimes Legislation Amendment (National Investigative Powers and Witness Protection) Bill 2006, which lapsed when the Parliament was prorogued in 2007.
Disclosure offences in other Australian jurisdictions

For completeness, the following comments relate to the controlled operations regime in various other Australian jurisdictions. The model controlled operations disclosure offence provision (clause 22, set out earlier), proposed that it would be an offence where a person:

- intentionally, knowingly or recklessly discloses information, and
- knows or is reckless as to whether the information relates to a [relevant, authorised] operation.

New South Wales, Victoria, Queensland and Tasmania have implemented this wording in their controlled operation laws.

Western Australia does not include a fault element and does not have an aggravated offence but instead applies the 10-year penalty to the basic offence.

The ACT limits the offence provisions to persons who are authorised to have the information and has different penalties depending on the type of harm: two years for prejudice to the effective conduct of an operation and 10 years for endangering the health or safety of any person.

Consistently with the model provision, all of the offences referred to above use the words ‘relates to’ or ‘relating to’ an operation.

The Northern Territory does not have a controlled operations regime in place.

South Australia has a controlled operations regime (under the Criminal Investigation (Covert Operations) Act 2009 (SA)) but did not implement the model provision and does not have a specific disclosure offence in this context.

The various relevant disclosure offence provisions are as follows:

- section 20R of the Law Enforcement (Controlled Operations) Act 1997 (NSW)
- section 36 of the Crimes (Controlled Operations) Act 2004 (Vic)
- section 266 of the Police Powers and Responsibilities Act 2000 (Qld)
- section 26 of the Police Powers (Controlled Operations) Act 2006 (Tas)
- section 35 of the Criminal Investigation (Covert Powers) Act 2012 (WA)
- section 26 of the Crimes (Controlled Operations) Act 2008 (ACT).
How does an SIO compare with a controlled operation?

An SIO is an operation that is carried out for a purpose relevant to the performance of one or more ‘special intelligence functions’ (see the definition of ‘special intelligence operation’ in section 4 of the ASIO Act).

A ‘special intelligence function’ means a function of ASIO under paragraph 17(1)(a), (b), (e) or (f) of the ASIO Act (see the definition in section 4 of the ASIO Act). These are, in effect, the various intelligence-gathering functions of ASIO (the functions not covered by the definition are ASIO’s advisory functions, including furnishing security assessments and providing advice relating to protective security).

ASIO’s function under paragraph 17(1)(f) of the ASIO Act is to cooperate with and assist bodies referred to in section 19A (that is, Australian Secret Intelligence Service (ASIS), Australian Signals Directorate (ASD), Australian Geospatial-Intelligence Organisation (AGO), a law enforcement agency (as defined) and an authority of the Commonwealth or of a State that is prescribed by regulations—of which there presently are none) in accordance with that section. Section 19A provides that ASIO may cooperate with and assist those bodies in the performance of their functions. This may involve obtaining intelligence which (unlike under ASIO’s other relevant functions) need not be linked with ‘security’. In doing so, ASIO’s legal and policy obligations continue to apply to those activities.

ASIO’s intelligence-gathering functions are primarily directed at obtaining intelligence that will help ASIO to protect Australia and its people from specified threats to ‘security’ (as defined in, and for the purposes of, the ASIO Act). This in part involves trying to predict emerging threats to security.

As such, the purpose of SIOs differs from that of controlled operations, which are primarily for law enforcement purposes, including obtaining the evidence needed to prosecute people alleged to have committed criminal offences.

The evidence obtained during controlled operations is intended to be, and often is, used in criminal court processes in an effort to obtain a conviction. As a result, the processes by which the evidence was obtained may be subjected to judicial scrutiny. By comparison, ASIO activities are generally conducted in secrecy by necessity, due to the nature of security intelligence work, and SIOs in particular are intended, generally, to remain secret in perpetuity.

There are some circumstances in which intelligence gathered by ASIO may be used in legal proceedings, including in a prosecution (the SIO scheme contemplates this
in sections 35A, 35P and 35R). Further, the Government and Parliament appear to increasingly expect ASIO to work closely with law enforcement agencies, particularly in counter-terrorism matters. Together with the tendency for the criminal law increasingly to apply to preparatory acts connected with acts of terrorism, rather than being limited to terrorist acts as such, this is one basis used to justify the SIO scheme. In other words, an SIO scheme is necessary to alleviate the increasing risk, for example, that covert conduct by ASIO employees and ASIO affiliates may expose them to prosecution.

Nonetheless, the purpose of the SIO scheme differs from that of the controlled operations scheme because the former relates to ASIO’s statutory functions. Further, ASIO’s intelligence-gathering functions extend beyond the counter-terrorism context (to include, for example, intelligence related to espionage, sabotage and acts of foreign interference). This means that SIOs may also be used in other settings. The SIO scheme is also available, for example, to counter the actions and activities of foreign state and non-state actors contrary to the interests of Australia and which may also constitute offences against Australian law. In this context also, covert conduct by ASIO employees and ASIO affiliates may involve unlawful activities.
Appendix L—History of Commonwealth secrecy offences

Outline

This appendix briefly sets out the history of secrecy offences relevant for this inquiry, with a focus on:

- the main relevant general Commonwealth secrecy offences, namely sections 70 and 79 of the *Crimes Act 1914* (Crimes Act)
- the agency-specific offences created later in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) and the *Intelligence Services Act 2001* (IS Act), and
- a proposed general secondary disclosure offence, which has not as yet been implemented.

Discussion

General secrecy offences in the Crimes Act

When first enacted, the *Crimes Act 1914* (No 12 of 1914) contained:

- Part VI (Offences by and against public officers), sections 70–76, and
- Part VII (Breach of official secrecy), sections 79–85.

Section 70 (Disclosure of official secrets) and section 79 (Unlawful communication of secret information) were among the provisions.

Section 70 (then, as now) adopts a ‘catch-all’ approach to prohibiting the unauthorised disclosure of official information (subject to the person being under a duty of non-disclosure).

Section 70 was modelled on section 86 of the Queensland *Criminal Code 1889*.

Section 70 today retains the same basic structure it had originally, apart from being extended in 1960 (see below) to apply to former Commonwealth officers.

Section 79 today retains the same basic structure it was given in 1960 (see below).

Section 79 was based on provisions of the *Official Secrets Act 1911* (United Kingdom).
ASIO established
ASIO was established on an executive basis by Prime Minister Chifley on 16 March, 1949.\(^{57}\)

Petrov Royal Commission
The Petrov Royal Commission (the Royal Commission on Espionage, 1954–55), which was established by the Menzies Government, inquired into allegations of spying associated with the defection of Mr and Mrs Petrov, who had been working at the Soviet Embassy in Canberra.

The Commission pointed out that there was no section of the Crimes Act which dealt adequately with spying during peacetime.

ASIO placed on a statutory basis
ASIO was placed on a statutory basis by the Australian Security Intelligence Organization Act 1956 (No 113 of 1956), (the 1956 Act).

Changes to the Crimes Act in 1960
The Crimes Act 1960 (No 84 of 1960) repealed and substituted sections 70 and 79 of the Crimes Act.

Section 70 was extended to apply to former Commonwealth officers.

Section 79 was extended by describing in a broad way the kind of information caught by the provision.

The penalties attaching to breaches of section 79 were made different, according to the gravity of the act constituting the breach—some new offences and express harm requirements were introduced to this end. (Section 79 previously contained only a ‘communication’ and a ‘retention’ offence, neither of which had an express harm requirement and which had the same penalty, of imprisonment for seven years.)

Section 78 (the precursor to section 91 of the Criminal Code, which was referred to in section 79) was made to apply in relation to a ‘foreign power’ as well as to an ‘enemy’, so that espionage would not be confined to spying during wartime.

---

\(^{57}\) This and other aspects of the history of ASIO and the ASIO Act are set out in more detail in Appendix H.
A relevant prosecution

*Grant v Headland* (1977) 17 ACTR 29 concerned the prosecution and conviction in the ACT Magistrates Court, affirmed on appeal by the ACT Supreme Court (for an offence against section 79(3) of the Crimes Act) of a probationary ASIO trainee, who communicated official secrets as part of what he alleged was a ‘personal practical experiment’ to see what kind of a response he would get to an overture to a foreign agency purporting to offer intelligence secrets. It was argued that the officer was unaware of any duty to keep the information secret, but it was held that a duty arose by necessary inference from the circumstances.

First Hope Royal Commission

The first Hope Royal Commission (the Royal Commission on Intelligence and Security, 1974–77), conducted by Justice Robert Hope, was instituted by the Whitlam Government—the first Labor Government to take office since the Petrov affair. Among other things, the Commission discussed:

- the need for further controls over the communication of ASIO information, and
- the importance of human sources to ASIO, stating that it was critical that the identity of human sources be protected. \(^58\)

The ASIO Act

The 1956 Act was repealed and replaced by the much more detailed *Australian Security Intelligence Organization Act 1979* (ASIO Act), with effect from 1 June 1980. The ASIO Act was to a large extent based on the recommendations made by the first Hope Royal Commission.

Second Hope Royal Commission and related changes

The Second Hope Royal Commission (the Royal Commission into Australia’s Security and Intelligence Agencies, 1983–85) was instituted by the Hawke Government following the Combe/Ivanov affair. Among other things, the Commission discussed the assessment and communication of intelligence and the scope of section 92. \(^59\)

Review of Commonwealth criminal law (Gibbs Committee)


---

\(^{58}\) See Appendix H for more details.

\(^{59}\) See Appendix H for more details.
the general secrecy offences in the Crimes Act, not agency-specific secrecy offences.

Litigation in the United Kingdom and Australia associated with the publication of *Spycatcher*, the memoirs of Peter Wright, a former member of the British security service who had moved to Australia to live, appears to have been a major part of the background to the Gibbs Committee consideration of secrecy offences. Several of these cases are discussed in some detail (including one decided post-report, included in an addendum). Paragraph 25.32 of the report states:

> Recent events indicate that consideration must be given to the possibility of a person in possession of official information, the disclosure of which could cause real harm to the public interest, departing from Australia and then publishing the information abroad.

The Gibbs Committee said the following (paragraph 25.12) in relation to significant existing secrecy offences:

> The combined effect of sections 70 and 79 is that the unauthorised disclosure of most information held by the Commonwealth Government and its agencies is subject to the sanctions of the criminal law. No distinction is drawn for the purposes of these provisions between information the disclosure of which may cause real harm to the public interest and information the disclosure of which may cause no harm whatsoever to the public interest.

The Gibbs Committee summarised (paragraph 25.42) the limitations on the operation of existing Australian law in regard to information, the disclosure of which could cause real harm to the public interest, as follows:

- A prosecution of a subsequent publisher for breaches of sections 70, 79 or 5 (ancillary offences, eg, aid and abet) of the Crimes Act will ordinarily not succeed without proof of the identity of the officer who made the disclosure, the channel of communication to that publisher or at least the circumstances under which the publisher received the information in question.
- Injunctive proceedings for breach or feared breach of those provisions are not available.
- An injunctive proceeding for breach of copyright will not succeed if the publication does not reproduce the form of the original document.
- Injunctive proceedings based on breach of confidence will not succeed if there has been any prior publication. Further, circumstances may well arise where the authorities have no notice or insufficient notice of intended publication of
matters in breach of confidence to enable them to apply for an injunction before publication.

- Section 18 of the ASIO Act has no application outside Australia and its external territories.60
- Failing some international agreement, there is doubtful prospect of enforcing in a foreign court any civil obligations of confidence in respect of unauthorised publication outside Australia of official information acquired in Australia.

The Gibbs Committee stated, by way of broad summary (paragraphs 24.5–24.7), that the report recommends the United Kingdom Official Secrets Act 1989 be broadly followed, with some modifications in the interests of broader access to information concerning government. In particular:

- the Committee recommends a defence of prior publication not present in the United Kingdom model, and
- the Committee has recommended protection in certain circumstances for whistleblowers and there is no corresponding provision in the United Kingdom Act.

The Gibbs Committee made relevant recommendations as follows (in Chapter 35), and further details were provided in a draft Bill to amend the Crimes Act annexed to the Committee’s report:

- The ‘catch-all’ provisions of section 70 and section 79(3) of the Crimes Act be repealed and replaced with provisions under which penal sanctions attach to unauthorised disclosure of official information should be limited to information in specified categories, including information:
  - relating to the intelligence and security services
  - relating to defence
  - relating to foreign relations, and
  - obtained in confidence from other governments or organisations.
- In the case of information relating to defence, relating to foreign relations and information obtained in confidence from other governments or organisations, the prosecution be required to prove that the disclosure caused damage.

60 This particular limitation was removed by amendments of the ASIO Act made by the NSLA Act (No 1) 2014. Section 18C of the ASIO Act provides that section 15.4 of the Criminal Code (extended geographical jurisdiction-category D) applies to an offence against section 18, 18A or 18B. Section 35P(4) makes similar provision in relation to an offence against section 35P of the ASIO Act.
• In the case of intelligence relating to the intelligence and security services, the prosecution would not have to prove damage, but would have to prove damage if the disclosure was made by a person who was not a member or ex-member of those services.
  – This recommendation was subject to the proviso that satisfactory procedures are established to receive, investigate and deal with complaints or allegations by members and ex-members of the services about illegality, misconduct or improper activities by those services, or persons the services employed.

  (In other words, a ‘whistleblower’ scheme.)

• It should be a defence for a person charged with an offence under the proposed provisions where proof of damage is required that he or she did not know and had no reasonable cause to believe that the information related to the matters in question or that its disclosure would be damaging.

• It should be provided that the proposed provisions could be enforced by injunction at the suit of the Attorney-General, but this would be subject to the same requirements of proof of harm as applied in a prosecution.

• Where a person knows or has reasonable grounds to believe that information:
  – had been disclosed (whether to him or her or another) by a Commonwealth officer or government contractor without authority or had been unlawfully obtained from either such person, or
  – had been entrusted to him or her in confidence by such officer or contractor on terms requiring it be held in confidence, or
  – had been disclosed (whether to him or her or another) without lawful authority by a person to whom it had been entrusted

it would be an offence for the person to disclose the information without authority, knowing or having reasonable cause to believe that the disclosure would be damaging.

• There should be a defence of prior publication (not available to a member or ex-member of the intelligence and security services in respect of information available to him or her in that capacity), which would require the defendant to satisfy the court:
  – that the information in question had previously been published
that, having regard to the nature and extent of that prior publication and the place where it occurred, the defendant had reasonable grounds to believe that the second publication was not damaging, and

- the defendant was not in any way directly or indirectly involved in the prior publication.

- The defence of public interest should not be provided for.

- However, where an employee or contractor of the Commonwealth or a Commonwealth agency reasonably believes that information in his or her possession evidences:
  - an indictable offence against a law of the Commonwealth, State or Territory
  - gross mismanagement or a gross waste of funds, or
  - a substantial and specific danger to public health or safety

he or she may, regardless of any requirement of law, disclose that information...

- in the case of a member of the intelligence or security services, to the Inspector-General of Intelligence and Security.

- It should be an offence for a person:
  - with knowledge that he or she is acting without proper authority to communicate any official information to any other person, knowing that such communication is likely to harm the safety or defence of Australia, or
  - to obtain unlawfully official information with a view to communicating it to another person, knowing that such communication was likely to harm the safety or defence of Australia.

(‘Official information’ to be defined to mean:

- information held by a department or agency of the Commonwealth
- information in the possession of an officer by virtue of his or her office
- information which had been information of those kinds but which had been unlawfully obtained from the officer or body in question, or
- had been disclosed without authority.)
Constitutional implied freedom of political communication
In a series of cases beginning in 1992, the High Court has held that the Australian constitution contains an implied freedom of political communication (see Appendix J for further discussion of this subject).

A relevant prosecution
In 1994 ASIO officer George Sadil was committed for trial in the ACT Magistrates Court for several offences under the Crimes Act relating to espionage and the disclosure of official secrets. The more serious espionage-related charges were discontinued by the prosecuting authorities, but Sadil pleaded guilty later in 1994 to summary charges of removing ASIO documents contrary to his duty.

Commission of Inquiry into ASIS
Some media reports concerning ASIS and its officers during 1993 and 1994 led to the establishment of a Commission of Inquiry into the operations and management of ASIS.

The public report of the ASIS Inquiry 1995 (conducted by the Hon Gordon Samuels and Mr Michael Codd) discusses in some detail relations between ASIS and the media. It contains chapters dealing with:

- the protection of sources and methods
- civil remedies to prevent unauthorised disclosure
- criminal sanctions against publication, and
- the public face of ASIS.

The Commission considered that:

- legislation to affirm the existence of ASIS and to provide authority for its activities was desirable in principle and would be of benefit in practice, and
- if the Parliament gave statutory authority to ASIS, it should be able to review the manner in which that authority is exercised (via a parliamentary committee).

The Commission stated the following in the summary to the public report:

- There is value in the maintenance of a voluntary D Notice system which, however, requires reinvigoration.
- The Commission supported the approach of the Gibbs Committee to the amendment of the Crimes Act but did not agree that proof of damage should be dispensed with in every case where information is disclosed by

---

Independent National Security Legislation Monitor | 138
an officer or former officer (rather, in such cases proof of damage should be required save where the likelihood of harm is overwhelming, for example, disclosure of current operations).

- The Commission supported the Committee’s recommendation on protection of whistleblowers and also recommended the provision of a public interest defence.

- The Commission supported the Committee’s recommendation about secondary disclosure, but because this provision would apply most often to journalists, such a change should not be made until the restored D-Notice system has been given a chance to function.

- The Commission also recommended that a provision akin to section 92 of the ASIO Act be included to protect present and former officers and sources against disclosure of their identities:

  - In this context, the Commission did not consider there was any need for proof of damage.

(The Commission did not discuss the fact that section 92 applies to any person and thus, operates in relation to ‘secondary’ disclosures.)

**Government response to the ASIS inquiry**

The Australian Government (through the Minister for Foreign Affairs, Senator Gareth Evans) relevantly responded as follows to the Commission, on 1 June 1995\(^61\) (this is a summary):

- The Government agreed that ASIS should be placed on a statutory basis and proposed to introduce legislation at the earliest practical opportunity.

- The most important measures available to prevent and punish the disclosure of sensitive national security information are the official information provisions in the Crimes Act, which were reviewed by the Gibbs Committee (the Government’s final consideration of which is awaiting the finalisation of the response to a Senate Committee report, tabled on 30 August 1994, on public interest whistleblowing).

- The Government was firmly of the view that in the areas of intelligence and security, defence and foreign relations the criminal provisions relating to the disclosure of official information need to be redesigned to overcome the problems of imprecision and potential overreach involved in the applications of sections 70 and 79 of the Crimes Act.

---

\(^61\) *Hansard*, Senate, Thursday 1 June 1995 (pages 716–726).
• The Government position in this respect differed from both the Gibbs Committee and the Commission, and involved the following basic elements:
  - Descriptions, as full as possible, of the kinds of disclosures of security information which are prohibited.
  - Liability to extend not only to disclosures by members and former members of the intelligence and security services and other relevant officials, but to ‘secondary’ disclosures. (The Government did not propose to defer this to give the D-Notice system time to work, on the basis that this does not take account of the fact that the proposed offences would be applicable beyond the recipients of D-Notices. Failure to provide criminal sanctions in relation to secondary disclosures could make the sanctions on primary disclosure quite ineffective.)
  - The Government to be required to prove damage or likely damage in all cases.
  - Illegality under Australian law of an act the subject of a disclosure to be a defence to prosecution.

The Parliament did not enact legislation giving effect to the proposed changes prior to the 1996 general election, which resulted in a change of government.

The Government indicated that it would, in consultation with the media, reinvigorate the D-Notice system. However, it added that, if the media did not understand or accept the underlying need for secrecy, or was unable to distinguish between those disclosures which are likely to be damaging and those which are not, any system of voluntary restraint was likely to have mixed success.

**In Confidence Report**
The report, entitled *In confidence—A report of the inquiry into the protection of confidential personal and commercial information held by the Commonwealth*, by the House of Representatives Standing Committee on Legal and Constitutional Affairs, was tabled in June 1995.

The relevant inquiry was quite general and did not deal in any detail with secrecy offences as they relate specifically to national security matters. However, the Committee did make the following comments and recommendation in relation to secondary disclosure of relevant material by the media:
7.11.7 The Committee has long been an advocate of protecting the rights of the accused. It believes that a decision to reverse the onus of proof should only be made in exceptional circumstances. However, the Committee also recognises the need to protect third party interests. In balancing these concerns, the Committee considers that an innocent recipient of confidential information should not be liable to prosecution by reason only of possession of the information. However, criminal liability should attach if that person has the requisite mental element and proceeds to use, disclose or make a record of the confidential information. This applies equally to second, third and later recipients in the distribution chain.

... 

7.11.10 The Committee finds it difficult to see why confidential third party information published by the media should not be subject to criminal sanctions when the persons previously involved in the distribution chain would be subject to such sanctions. The Committee considers that there is no justification for a public interest defence in these circumstances.

*Recommendation 31*

The Committee recommends that unauthorised dealing in confidential third party information held by the Commonwealth and its agencies, should be prohibited at every point on the distribution chain by general offence provisions in the *Crimes Act 1914*.

**The Intelligence Services Act**

The recommendations of the Commission of Inquiry into ASIS ultimately led to the passage of the *Intelligence Services Act 2001* (IS Act) which, among other things:

- set out the functions and governed the activities of ASIS and the Defence Signals Directorate, or DSD (now the Australian Signals Directorate, or ASD) (sections 6 and 7)
- established a parliamentary committee (now the Parliamentary Joint Committee on Intelligence and Security) to review the administration and expenditure of, and certain other matters relating to, ASIO, ASIS and DSD (section 29)
- created secrecy offences, applicable to current and former officials and other ‘insiders’ of those agencies akin to section 18 of the ASIO Act in relation to ASIS and DSD (sections 39 and 40).
(As a consequence of the Intelligence Services Legislation Amendment Act 2005 (No 128 of 2005), as of 2005 the IS Act applied in similar fashion to the Defence Imagery and Geospatial Organisation or DIGO (now the Australian Geospatial-Intelligence Organisation, or AGO). Section 39A contains the equivalent secrecy offence.)

- included a secrecy offence akin to section 92 of the ASIO Act relating to ASIS officials and agents (section 41), applicable to any person and requiring no proof of damage (However, unlike section 92 of the ASIO Act, this offence had extra-territorial application) and
- did not otherwise include a secrecy offence applying to secondary disclosures.

**Proposed relevant changes to the Crimes Act**

In 2001, the Australian Government introduced a Bill into the Parliament (the Criminal Code Amendment (Espionage and Related Offences) Bill 2001) which would have repealed Part VII of the Crimes Act (including section 79) and created new offences in relation to official secrets in proposed Division 82 of the *Criminal Code*:

- A modified version of the Bill, the Criminal Code Amendment (Espionage and Related Offences) Bill 2002 was introduced into the Parliament in 2002 and this later became law. This later Bill omitted most of the official secrets changes because of the criticism they attracted. The only change made to these provisions was to replace the phrase ‘safety or defence’ with ‘security or defence’.
- According to *Bills Digest No 117 2001-02*, relating to the later Bill, while the 2001 Bill did not significantly change the law on official secrets, this aspect of the Bill was heavily criticised particularly in the press for containing gaol terms for secondary disclosure or ‘whistleblowing’ in relation to non-national security matters, even when the information was disclosed or published on so-called public interest grounds. An appendix to this *Bills Digest* related to the Lappas case (summarised below).
- The new provisions did not replicate the existing ones. In particular, that the offence of ‘receiving certain information’ (proposed clause 82.4 of the *Criminal Code*) did not require the person to know or have reasonable grounds to believe that the information was communicated in contravention of the espionage or secrecy provisions.
A relevant prosecution
In July 2000 Simon Lappas, a former Defence Intelligence Organisation (DIO) analyst, was charged with official secrets offences under section 79 of the Crimes Act. Additional espionage charges were brought under section 78(1)(b) of the Crimes Act in 2001. It was alleged that Lappas gave several classified documents to another person who was not authorised to receive them, so that she could sell them to a foreign power.

The Lappas case was long and complex and formed part of the background to the ALRC inquiry, discussed below, which led to Report 98, Keeping Secrets (The Protection of Classified and Security Sensitive Information). Appendix 4 to that report discusses the case. Lappas was ultimately convicted and incarcerated for a period following a successful appeal by the Crown to the Court of Appeal of the Supreme Court of the ACT against the sentence imposed (see R v Lappas [2003] ACTCA 21 and R v Lappas and Dowling [2001] ACTSC 115).

A secrecy offence related to warrants and questioning
The secrecy offence in section 34VAA was added to the ASIO Act by the ASIO Legislation Amendment Act 2003 (No 143 of 2003). This offence potentially applies to any person and involves the disclosure of information that relates to certain warrants and questioning powers associated with countering terrorism.

Section 34VAA of the ASIO Act was repealed and replaced by the secrecy offence in section 34ZS, which was added by the ASIO Legislation Amendment Act 2006 (No 54 of 2006).

These offences involve information (put broadly):

- which indicates a fact relating to a relevant warrant or that a warrant has been issued, or
- which is ‘operational information’, defined broadly but which, if the first limb is inapplicable, the discloser must have as a direct or indirect result of the warrant.

The Bennett case
In 2003, the Federal Court (Finn J) held in Bennett v President, Human Rights and Equal Opportunity Commission (2003) 134 FCR 334 that regulation 7(13) of the Public Service Regulations was invalid because it was contrary to the constitutional implied freedom of political communication. (See Appendix J for further discussion of this subject.)
ALRC report 98
The Australian Law Reform Commission (ALRC) provided ALRC report 98, *Keeping Secrets (The Protection of Classified and Security Sensitive Information)*, to the Government in 2004. This inquiry involved a review of the handling and protection of classified and security-sensitive information in legal proceedings (a subject dealt with in part by the *National Security Information (Criminal and Civil Proceedings) Act 2004*, which was then a Bill, referred to by the ALRC).

Chapter 5 of that report deals with ‘Prevention and punishment of unauthorised disclosure’ and contains the following recommendations:

- Sections 70 and 79 of Crimes Act and section 91.1 of the *Criminal Code* should be amended to provide that, where the courts are satisfied that a person has disclosed or is about to disclose classified or security sensitive information in contravention of the criminal law, the courts may grant an injunction to restrain such disclosure or further disclosure.
  
  (The subject ‘Restraining a breach of the criminal law’ including relevant comments made by Mason J in *Commonwealth v Fairfax* (1980) 147 CLR 39 are discussed in paras 5.25–5.36 of the report.)

- The Australian Government should review all legislative and regulatory provisions giving rise to a duty not to disclose official information—including in particular regulation 2.1 of the Public Service Regulations—to ensure that the duty of secrecy is imposed only in relation to information that genuinely requires protection and where unauthorised disclosure is likely to harm the public interest.

- In conducting the review proposed above, the Australian Government should ensure that a clear distinction is drawn between conduct that gives rise to administrative sanctions under the public service legislation and conduct that gives rise to criminal sanctions, including those under section 70 of the Crimes Act.

- The Australian Government should undertake a comprehensive review of section 79 of the Crimes Act in order to clarify and modernise the language and intent of the provision and to ensure that an appropriate public policy balance is found across the range of offences created by the provision.
  
  Such a review should consider, among other things:

  - the possible need for a new summary offence of strict liability dealing with the unauthorised disclosure of classified information and attracting a maximum penalty of no more than 12 months’
imprisonment—and including certain safeguards, such as defences of due diligence and reasonable mistake
- the need to limit certain offences to circumstances in which disclosure of the information is likely to, or did in fact, harm the public interest, and
- the relationship of section 79 with section 70 of the Crimes Act and section 91.1 of the Criminal Code.

- The Australian Government should undertake a review of Commonwealth secrecy provisions to ensure that:
  - each provision is consistent with the Constitution, and
  - all provisions are broadly consistent, allowing for any reasonably necessary variation among agencies.

**ALRC report 112**

The ALRC was itself tasked by the Government in 2008 with conducting a comprehensive review of Commonwealth secrecy laws. ALRC report 112, *Secrecy Laws and Open Government in Australia*, was provided to the Government in December 2009.

One major reform recommended in this report, the creation of a general Commonwealth secrecy offence to replace many of the existing offences, has not been implemented. The report contains many recommendations and a wealth of discussion that is of significance for the purposes of this inquiry. Some of the relevant recommendations, focusing on matters discussed above, are as follows. (In reading the following, it is important to note that the ALRC accepted that there was a case for specific secrecy offences in relation to intelligence and security agencies, and that the ALRC was here referring to offences applicable to insiders. The ALRC makes it plain, for example (see paras 8.62–8.63 and 9.129 of the report), that persons outside the Australian Intelligence Community or AIC cannot be expected to have a similar level of knowledge or responsibility as officers within of the AIC and others who work in and with such agencies. Those within the intelligence community have special duties and responsibilities.):

- Sections 70 and 79(3) of the Crimes Act should be repealed and replaced by new offences in the Criminal Code—the ‘general secrecy offence’ and the ‘subsequent disclosure offences’. (Recommendation 4-1)
- The general secrecy offence and the subsequent disclosure offences should provide that, where a court is satisfied that a person has disclosed, or is about to disclose, information in contravention of the provisions, the court
may grant an injunction to restrain disclosure of the information. (Recommendation 7-6)

- Specific secrecy offences that apply to individuals other than Commonwealth officers should clearly identify the parties regulated by the offence. (Recommendation 8-1)

- Specific secrecy offences should include an express requirement that, for an offence to be committed, the unauthorised disclosure caused, or was likely or intended to cause, harm to an identified essential public interest, except where:
  - the offence covers a narrowly defined category of information and the harm to an essential public interest is implicit, and
  - the harm is to the relationship of trust between individuals and the Australian Government integral to the regulatory functions of government. (Recommendation 8-2)

- Specific secrecy offences that apply to Commonwealth officers should also apply to former Commonwealth officers. (Recommendation 9-2)

- Specific secrecy offences should generally require intention as the fault element for the physical element consisting of conduct. Strict liability should not attach to the conduct element of any specific secrecy offence. (Recommendation 9-4)

- Specific secrecy offences with an express harm requirement should generally require that a person knew, intended that, or was reckless as to whether, the conduct would cause harm to an essential public interest. (Recommendation 9-5)

- Specific secrecy offences without an express harm requirement should require that a person knew, or was reckless as to whether, the protected information fell within a particular category, and should not provide that strict liability applies to that circumstance. (Recommendation 9-6)

- Offences for the subsequent unauthorised disclosure of information should require that:
  - the information has been disclosed in breach of a specific secrecy offence
  - the person knows, or is reckless as to whether, the information has been disclosed in breach of a specific secrecy offence, and
  - the person knows, intends or is reckless as to whether the subsequent disclosure will harm—or knows or is reckless as to whether the subsequent disclosure is reasonably likely to harm—a specified essential public interest. (Recommendation 9-7)
A relevant prosecution
ASIO officer James Sievers was prosecuted in 2009 for an offence against section 18(2) of the ASIO Act. His co-accused, Francis O’Ryan, was charged with aiding and abetting or procuring the offence, in accordance with section 11.2(1) of the Criminal Code. An earlier trial in 2008 (the relevant events occurred in 2004) had been aborted after the jury failed to agree on a verdict. The convictions against both accused were ultimately set aside by the Court of Appeal of the Supreme Court of the ACT (see Sievers v R [2010] ACTCA 9, in relation to Sievers), effectively because the prosecution had not established that there was no compelling evidence to enable the reasonable hypothesis advanced by the defence to be safely rejected. (The hypothesis was that O’Ryan had found ASIO documents in premises he shared with Sievers and had acted alone in communicating them to media interests.)

A secrecy offence related to controlled operations
The secrecy offence in sections 15HK and 15HL of the Crimes Act (the offences relating to controlled operations conducted by the Australian Federal Police (AFP), on which section 35P of the ASIO Act was modelled) were added by the Crimes Legislation Amendment (Serious and Organised Crime) Act 2010 (No 3 of 2010). (See Appendix K for further discussion of this subject.)

Significant disclosures of national security information
In 2010, United States Army Private Bradley (now Chelsea) Manning disclosed a large number of classified and unclassified sensitive military and diplomatic documents to Wikileaks. Many of these were made public by Wikileaks later in 2010.

In 2013, Edward Snowden, an American working for a contractor to the National Security Agency (NSA), disclosed thousands of classified NSA documents to a range of journalists. Many of these have subsequently been published by The Guardian newspaper and other media interests, including the Fairfax press in Australia.

The Public Interest Disclosure Act 2013
The main provisions of the Public Interest Disclosure Act 2013 (PID Act) came into operation on 15 January 2014. The PID Act provides a scheme for protection of certain public interest disclosures made by public officials (including ‘whistleblowers’). (See Appendix I for further discussion of this subject.)
The National Security Legislation Amendment Act (No 1) 2014

Section 35P, the secrecy offence which is the subject of the present inquiry, was added to the ASIO Act by the National Security Legislation Amendment Act (No 1) 2014 (the NSLA Act (No 1) 2014). In addition to this change, the NSLA Act (No 1) 2014 also made the following other relevant changes:

- increased the penalty for an offence against section 18(2) of the ASIO Act from imprisonment for two years to imprisonment for 10 years
- extended aspects of the IS Act to the remaining agencies forming the Australian Intelligence Community (AIC), namely the Defence Intelligence Organisation (DIO) and the Office of National Assessment (ONA) by
  - extending parliamentary (PJCIS) oversight to DIO and ONA, and
  - creating secrecy offences under the IS Act akin to section 18(2) of the ASIO Act in relation to DIO and ONA (sections 40B and 40A respectively) with penalties of imprisonment for 10 years
- increased the penalty for an offence against the secrecy offences under the IS Act (akin to section 18(2) of the ASIO Act) in relation to ASIS, ASD and AGO from imprisonment for two years to imprisonment for 10 years
- created new offences applicable in relation to all AIC agencies (with penalties of imprisonment for three years) for compromising intelligence information in ways that need not involve disclosure, namely for:
  - ‘Unauthorised dealing with records’ (section 18A of the ASIO Act, sections 40C, 40E, 40G, 40J and 40L of the IS Act), and
  - ‘Unauthorised recording of information or matter’ (section 18B of the ASIO Act, sections 40D, 40F, 40H, 40K and 40M of the IS Act)
- applied section 15.4 of the Criminal Code (extended geographical jurisdiction-category D) to the various new protection of information offences (and to section 18 of the ASIO Act)
- increased the penalty for an offence against section 92 of the ASIO Act (and section 41 of the IS Act, in relation to ASIS) from imprisonment for one year to imprisonment for 10 years and
- changed the employment provisions of the Act, with section 92 now applying in relation to making public the identity of a current or former ASIO employee or ASIO affiliate:
  - previously section 92 applied in relation to making public the identity of a current or former officer, employee or agent of ASIO.
(Paragraph 765 of the Explanatory Memorandum to the NSLA Bill (No 1) explains the difference between ASIO affiliates and (other) ASIO insiders for the purposes of the offences in sections 18–18B of the ASIO Act (specifically ‘entrusted persons’ for sections 18A and 18B). It states:

The term ‘entrusted person’ includes persons who have entered into a contract, agreement or arrangement with ASIO other than as an ASIO affiliate, to ensure that the offence in subsection 18A(1) applies to persons whose contract, agreement or arrangement is not for the performance of functions or services for the Organisation. This may include, for example, persons (such as officers of other Commonwealth agencies) who have received a security briefing to receive classified information from, prepared by, or pertaining to, the Organisation. Security briefings may be used as a pre-requisite to a person’s receipt of records or information from, prepared by or pertaining to the Organisation. Such briefings can require a person to agree to certain terms on which the records or information are to be provided. These include conditions on the person’s use, handling and disclosure of such records or information.
Appendix M—Existing Commonwealth secrecy offences: official comments

This appendix contains extracts from the extensive comments in relation to protection of information provided by the Attorney-General’s Department (AGD) and ASIO in the context of parliamentary processes related to the National Security Legislation Amendment Act (No 1) 2014 (NSLA Act (No 1) 2014).

The comments relate to the adequacy of the existing Commonwealth secrecy offences. Some of that discussion relates to what became Schedule 6 to the NSLA Act (No 1) 2014 (Protection of information) and some relates to what became Schedule 3 (the SIO scheme including section 35P).

The following extract is from the AGD response (dated 18 August 2014) to several matters taken on notice during the course of evidence given to the PJCIS on 15 August 2014:

**Schedule 3—special intelligence operations—secrecy offences**

**Justification for the offences in proposed s 35P**

**Committee questions**

Committee members asked Departmental and ASIO witnesses to provide further information about the need for the proposed new offences in relation to the communication of information relating to a special intelligence operation. In particular, further information was sought about why existing non-disclosure offences were considered insufficient or inadequate to cover such actions.

**Departmental response**

Further to the evidence of Departmental witnesses at the public hearing on 15 August, the Department provides the following additional observations about limitations in other, existing criminal offences that could potentially apply to some instances of conduct that would constitute an offence against proposed s 35P.

These limitations arise principally because existing offences are directed to different forms of mischief to that which is targeted by proposed s 35P, with the result that their physical elements may not apply, or they would not adequately target and denounce the wrongdoing associated with compromising a covert intelligence operation that is of sufficient importance to have been designated as...
a special intelligence operation, in accordance with the authorisation process set out in Schedule 3 to the Bill.

**Offences under the ASIO Act**

In particular, the existing offence in s 18(2) of the ASIO Act concerning the unauthorised disclosure of intelligence-related information (including with the amendments proposed in Schedule 6 to the Bill) applies to persons who are in a specified form of relationship with ASIO (by way of employment, contract, agreement or some other form of arrangement).

While this may cover participants in special intelligence operations, and others within ASIO or other agencies who are legitimately privy to details of such operations, it may not cover persons to whom such information is disclosed on an unauthorised basis, and who engage in subsequent disclosures. This is a considerable limitation, given that the disclosure of the existence of a covert intelligence operation is, by its very nature, prejudicial to the effectiveness or viability of that operation. Such disclosure additionally carries a substantial risk of endangering the lives or safety of participants, who are likely to have close contact with persons of security concern as part of the operation.

The wrongdoing targeted by s 35P is the harm that is occasioned by the very fact of disclosure of information about a special intelligence operation. Therefore, the nature of a person’s prior relationship (if any) with ASIO is not necessarily material to a person’s culpability (although it may be a relevant consideration in sentencing a person convicted of an offence against s 35P). Relying on the existing offence in the ASIO Act would not, therefore, adequately target or contribute to deterring the wrongdoing to which proposed s 35P is directed.

A further offence under s 92 of the ASIO Act, concerning the publication of the identity of an ASIO officer (which is proposed to be amended by Schedule 1 to the Bill to adopt the terminology of an ASIO employee or an ASIO affiliate rather than an ‘officer’) could potentially apply to persons who communicate information relating to a special intelligence operation.

However, this offence will only be open if the relevant information communicated about the special intelligence operation would disclose the identity of an ASIO officer or an ASIO affiliate. This may not cover all participants in a special intelligence operation, and would not offer any protection against the disclosure of other information about the operation. In addition, the offence carries a maximum penalty of imprisonment for one year, which is disproportionate to the harm associated with conduct that—in addition to disclosing an ASIO officer or affiliate’s identity—will prejudice a special intelligence operation by disclosing its
existence, and may place at risk the lives or safety of participants, or persons connected to such participants.

Offences in the Criminal Code

Other criminal offences in the nature of espionage in Division 91 of the Criminal Code 1995 (Cth) (Code) require proof of a person’s intention to cause a specified form of serious harm, such as prejudice to the security or defence of the Commonwealth (or that this was the likely result of the person’s conduct); or to give an advantage to another country’s security or defence (or that this was the likely result of the person’s conduct). The maximum penalties of 25 years’ imprisonment applying to these offences reflect that they are directed to conduct which causes, or is intended to cause, harm of the gravest possible nature to Australia’s security interests. While a person who disclosed information about a special intelligence operation with the requisite intention to cause harm of one of these kinds could potentially be prosecuted under Division 91 of the Criminal Code, these offences are targeted to harm at the very uppermost end of the spectrum. They are not of application to the comparatively lesser, but still highly significant, degree of harm that may be occasioned by unauthorised disclosures of information relating to special intelligence operations in the absence of any malicious intention on the part of the discloser, or with an intention to prejudice a particular operation or the health or safety of an individual.

The Department is aware that some submitters to the inquiry have identified other offences in the Criminal Code as being potentially relevant to the communication of information about a special intelligence operation, including treason (s 80.1) and materially assisting enemies (s 80.1AA). The prospects that these offences may have application in relation to the disclosure of information about special intelligence operations are, in the Department’s view, remote other than in very exceptional cases. These offences require the causation of death or harm to the Sovereign, the Prime Minister or Governor-General, or the levying of war or an armed invasion (or preparatory conduct) against the Commonwealth, or the intentional engagement in conduct to assist an enemy engage in war against the Commonwealth. The penalties of life imprisonment applying to these offences reflect their exceptional nature.
Offences in the Crimes Act

The Department is further aware that some submissions to the inquiry have suggested that adequate coverage is provided by some offences in s 79 of the Crimes Act, which are directed to the disclosure of official secrets. They relevantly cover:

- the unauthorised communication or retention of certain information or records by a person to whom it is entrusted, with the intention of prejudicing the security or defence of the Commonwealth, under penalty of seven years’ imprisonment: s 79(2);
- the unauthorised communication of certain information or records in the absence of any intention to cause harm, under penalty of two years’ imprisonment: s 79(3);
- the unauthorised retention or failure to take reasonable care of certain information or records, in the absence of any intention to cause harm, under a penalty of six months’ imprisonment: s 79(4);
- the receipt of certain information, where the recipient has reasonable grounds to believe the communication was made in contravention of s 91.1 of the Criminal Code (espionage) under penalty of seven years’ imprisonment: s 79(5); and
- the receipt of certain information where the recipient has reasonable grounds to believe the communication was made in contravention of s 79(3) of the Crimes Act (see above), under penalty of two years’ imprisonment.

The Department notes that these offences would not adequately target the wrongdoing inherent in conduct that would constitute an offence against proposed s 35P, particularly the basic offence in proposed s 35P(1). The only offence that would capture conduct targeted by proposed s 35P(1) is that in s 79(3) of the Crimes Act, which carries a maximum penalty of two years’ imprisonment. This is disproportionately low to the disclosure of information that, by its very nature, will prejudice a covert intelligence operation and carries a risk of jeopardising the lives and safety of participants.

As noted above, such harm is inherent in a disclosure of information about a special intelligence operation, irrespective of a person’s subjective intention (or otherwise) in making the disclosure. A maximum penalty of two years’ would not provide a sentencing court with an adequate range within which to impose a sentence that reflects the gravity of the consequences of the conduct constituting the offence. As such, a two-year sentence applying to an offence of general application would be unlikely to serve as a significant deterrent to persons who may be contemplating communicating information relating to a special intelligence operation.
The Department’s supplementary submission will address similar contentions made in relation to the proposed offences in Schedule 6. (Namely, suggestions that s 79 of the Crimes Act, and various other offences, adequately cover the wrongdoing to which the proposed amendments are directed.)

**Corresponding offences for controlled operations in Part IAB of the Crimes Act**

The offences in proposed s 35P are identical in their elements to those in ss 15HK and 15HL of the Crimes Act, in relation to the unauthorised disclosure of information relating to a controlled operation. The Department re-iterates its oral evidence on 15 August that no issues have been identified in relation to the application of these offences to date—which have been in force since 2010—to journalists or others reporting on, or seeking to discuss publicly, matters of law enforcement or national security.

In addition, advice from law enforcement agencies is that media professionals have engaged effectively with them in seeking guidance or clarification about reporting on such matters, in order to avoid the risk of unintentionally compromising sensitive operations. Media professionals can similarly contact the Organisation on a publicly listed telephone number on the Organisation’s website. The media telephone line is staffed 24 hours.

The following extract (footnotes omitted) is from the joint supplementary submission of AGD and ASIO, adding to evidence already given to the PJCIS, including the above response of 18 August 2014, to matters taken on notice on 15 August 2014:

**Schedule 6—protection of information**

**Coverage of existing secrecy offences of general application**

**Submissions and evidence**

Some submitters and witnesses argued that there is “no demonstrable need” for the proposed new and amended offences in Schedule 6 to the Bill because the wrongdoing to which they are directed is covered adequately by existing secrecy offences of general application. The Gilbert + Tobin Centre of Public Law commented:

>[T]he government’s claim that there are ‘significant gaps’ in the law is simply not supported. There is a wide range of existing offences that could apply to the disclosure of classified information, including severe penalties for terrorism, espionage and treason, as well as other penalties for disclosing official secrets and the disclosure of
information by Commonwealth officers. And, contrary to the government’s suggestion that ‘no such offences exist’, many of these offences would also apply to the situation where a person merely possesses or retains information. Section 79 of the Crimes Act provides for a maximum penalty of seven years imprisonment where a person retains a classified document ‘when it is contrary to his or her duty to retain it’. Given this comprehensive array of existing offences, there is no demonstrable need to create a new ‘three-tier structure’ for regulating the disclosure of classified information.

**Departmental and ASIO comments**

The material issue before the Committee and the Parliament is whether the particular wrongdoing sought to be targeted by the measures in Schedule 6 to the Bill is meritorious of being singled out for the imposition of a dedicated criminal sanction. That is, the Parliament is called upon to decide whether conduct that compromises, or places at risk of compromise, intelligence-related information ought to be the subject of specific criminal offences and penalties in the manner proposed by Schedule 6.

As the Attorney-General’s remarks in his second reading speech on the Bill indicate, the Government has taken the view that intelligence-specific secrecy offences are needed to recognise the particular harm inherent in the compromise of intelligence-related information, which goes over and above the offences and penalties applying to the compromise of other types of official information of a confidential nature. The need for intelligence-specific secrecy offences was endorsed in 1976 by the Hope Royal Commission on Intelligence and Security, which led to the introduction of the unauthorised communication offence in s 18(2) of the ASIO Act. As Justice Hope commented in his Fourth Report:

> The intelligence held by ASIO ... is often highly prejudicial ... and its dissemination should be strictly controlled by legislation as well as ethical rules. The minimum controls which should be contained in the legislation are that the communication may only be made by the Director-General or by somebody authorised by him, either generally or in the particular matter; and that communication of any intelligence by an unauthorised person, or otherwise than for the purposes of the Act, should be prohibited. Persons who infringe these provisions or who authorise its infringement should be subject to severe penalties.

> It is true that legislation alone will not ensure that no-one with access to ASIO’s intelligence speaks out of turn. But the least that must be done ... is to prohibit and penalise it.

The Attorney-General’s second reading remarks, together with the commentary in the Explanatory Memorandum to the Bill, further outline the Government’s view that there are significant gaps in the coverage of existing intelligence-specific
secrécy offences in the contemporary security environment in two key respects – namely:

• the disproportionately low penalties (two years’ imprisonment) applying to the existing offences in the ASIO Act and the Intelligence Services Act which target the unauthorised communication of intelligence-related information by persons to whom it is entrusted; and

• the absence of offences directed specifically to persons who place intelligence-related information at risk of compromise, but whose conduct stops short of communication of that information.

Accordingly, the material issue is not that a survey of existing criminal laws might identify various offences of general application that could potentially apply—in particular fact scenarios—to the conduct constituting the proposed new or amended offences in Schedule 6. Rather, the focus of any useful analysis of existing offences is whether or not they adequately cover the particular form of wrongdoing sought to be addressed by those in Schedule 6. (That is, the compromising of intelligence-related information, or placing such information at risk of compromise.)

As indicated in the Department’s responses to the matters taken on notice at the hearing of 15 August, there are significant limitations in the range of existing secrecy offences of general application, insofar as they may apply to the unauthorised communication of intelligence-related information, or dealings with or the making of records of such information. Limitations in the key categories of general offences are discussed below.

Offences in the Criminal Code

The espionage offences in Division 91 of the Criminal Code require that a person must intend to cause a specified form of serious harm, such as prejudice to the security or defence of the Commonwealth (or that this was the likely result of the person’s conduct); or to give an advantage to another country’s security or defence (or that this was the likely result of the person’s conduct). The maximum penalties of 25 years’ imprisonment applying to these offences reflect that they are directed to conduct which causes, or is intended to cause, harm of the gravest possible nature to Australia’s security interests. They are not of application to the comparatively lesser, but still highly significant, degree of harm or risk that may be occasioned by unauthorised communication of intelligence-related information, or unauthorised dealings with records or recording of information, in the absence of a specific intent to cause harm. (Further issues in relation to a specific harm requirement are considered separately below.)
Similarly, while some submitters have suggested that other offences such as treason (s 80.1) and materially assisting enemies (s 80.1AA) and a range of terrorism offences in Part 5.3 may potentially be relevant, their application is limited to very specific fact scenarios. They do not squarely address the wrongdoing to which the Schedule 6 offences are directed.

Offences in the Crimes Act—Part VII

Some submissions to the inquiry have also suggested that adequate coverage is provided by offences in s 79 of the Crimes Act, which are directed to the disclosure of official secrets. They relevantly cover:

- the unauthorised communication or retention of certain information or records by a person to whom it is entrusted, with the intention of prejudicing the security or defence of the Commonwealth, under penalty of seven years’ imprisonment: s 79(2);
- the unauthorised communication of certain information or records in the absence of any intention to cause harm, under penalty of two years’ imprisonment: s 79(3);
- the unauthorised retention or failure to take reasonable care of certain information or records, in the absence of any intention to cause harm, under a penalty of six months’ imprisonment: s 79(4);
- the receipt of certain information, where the recipient has reasonable grounds to believe the communication was made in contravention of s 91.1 of the Criminal Code (espionage) under penalty of seven years’ imprisonment: s 79(5); and
- the receipt of certain information where the recipient has reasonable grounds to believe the communication was made in contravention of s 79(3) of the Crimes Act (see above), under penalty of two years’ imprisonment.

It is considered, however, that the maximum penalties applying to these offences are disproportionately low to the wrongdoing targeted by the offences in Schedule 6. (The issue of penalties is discussed separately below.)
Appendix N—SIOs and protecting information: international comparisons

Introduction and caveats

The following comments are based on, and to some extent drawn from, submissions to the inquiry (including but not limited to those made by the Australian Government agencies), together with some independent research.

The comments involve, or may assist in making some, broad comparisons between:

- Australia’s SIO scheme in Division 4 of Part III of the ASIO Act and the special secrecy offences in that scheme (section 35P), and
- the approach taken to authorising illegal acts, including by covert human sources including in an intelligence and security setting, and to protecting related intelligence information, in some other similar countries.

The comments focus on Australia’s key allies in the intelligence realm.

The discussion of protection of intelligence information focuses on secrecy offences, rather than on methods of engagement between government and media interests. However, at the end of this appendix there is a brief description of the DSMA-Notice (Defence and Security Media Advisory-Notice) System in the United Kingdom (a structured means of engagement between the United Kingdom Government and certain media interests) and of the history of the defunct Australian equivalent.

As with this inquiry generally, the focus is on ‘leaks’ by ‘insiders’ and the role of journalists in investigative reporting. However, similar issues may arise in relation to any proposed publication of information obtained through ‘hacking’ computers.

Comparing the approach taken to intelligence operations by different intelligence agencies, and relevant secrecy offences, is a difficult task even within Australia.

Making that kind of comparison at an international level is even more difficult and must involve various caveats.

In particular, different countries have different historical, constitutional and policy factors that affect how they deal with such matters. The institutional arrangements in these countries may also reflect such differences. As a result, rules governing intelligence agencies that have with a foreign security focus often differ from the
rules governing agencies with a domestic security focus, including those in Australia.

Further, any discussion of the legal regime of another country may suffer from a lack of awareness of all relevant laws and administrative instruments or policies and other factors, including the various bodies that may be related to national security. There may be differences in the way that courts approach the construction of legislation and review administrative action.

Nonetheless, a broad outline of the legal framework of other countries does offer an insight into potential solutions for the fundamental issues that such laws seek to resolve. Against that background, the following comments in relation to other jurisdictions are not intended to be comprehensive.

**Overview**

The United Kingdom, the United States and Canada have schemes that authorise illegal acts, including by covert human sources in an intelligence and security setting.

Each jurisdiction (like Australia) has a range of secrecy offences which could apply to the disclosure of certain information about such activities. However, none appears to have a secrecy offence, like section 35P, specific to such activities or the operations they may form part of.

The United Kingdom has one secrecy offence, section 39 of the *Terrorism Act 2000*, discussed further below, which applies in relation to a ‘terrorist investigation’, conducted by a constable. This may be the nearest direct comparison with section 35P, although there are significant differences between the provisions.

With the arguably exception of section 39 of the *Terrorism Act 2000*, the breadth of the language used in fixing the range of information to which section 35P of the ASIO Act applies (information which ‘relates to’ relevant operational activities) seems to be unique.

Many of the secrecy offences in these jurisdictions apply to some defined grouping of ‘insiders’ (such as employees or contractors of intelligence or security agencies) who make disclosures in breach of the limits of their authority and in many cases they require either an intention to cause harm or resultant harm.
In addition, a number of offences include defences by way of ‘reasonable excuse’ or that a disclosure was made in the public interest.

**The United Kingdom**

*Authorised illegal acts*

In the United Kingdom, law enforcement, security and intelligence agencies use the *Regulation of Investigatory Powers Act 2000* (RIPA) to authorise the use and conduct of covert human intelligence sources.

Section 29 of the RIPA:

- confers power to grant authorisations
- sets out the preconditions to the grant of an authorisation for the conduct or use of a covert human intelligence source, and
- sets out the scope of authorised conduct.

The Secretary of State may prohibit the authorisation of any conduct or use of covert human intelligence sources and may impose requirements additional to those expressly provided for in the Act.

The conduct that is authorised is any conduct that:

- comprises any such activities involving conduct or the use of a covert human intelligence source as are specified or described in the authorisation
- consists in conduct by or in relation to the relevant covert human intelligence source, and
- is carried out for the purposes of, or in connection with, the investigation or operation so specified or described.

Section 27 of the RIPA provides that:

- conduct shall be lawful for all purposes if an authorisation confers an entitlement to engage in that conduct on the relevant person and the conduct is in accordance with the authorisation, and
- a person shall not be subject to any civil liability in respect of certain specified conduct which is incidental to conduct that is lawful for all purposes.

The United Kingdom common law recognises that the participation of officials and sources in unlawful activity may be proper for the purpose of giving evidence so
long as another person is not induced to commit a crime (R v Birtles [1960] 1 WLR 1074). (In this respect, compare section 35K(1)(d) of the ASIO Act.)

Relevant United Kingdom agencies may, where necessary, rely on an authorisation under the RIPA as a basis for effectively opposing the prosecution of an official or source for unlawful conduct related to the authorisation.

Section 30 of the RIPA relevantly explains which public officials (prescribed in an order made under that section) may grant authorisations under section 29.

There is also a Code of Practice relating to the conduct or use of covert human intelligence sources, made under section 71 of the RIPA.

The RIPA does not provide for broad immunity for activities associated with a particular operation. Rather, the RIPA enables particular activities to be authorised. The RIPA governs a range of investigatory activities, the more intrusive of which (such as interception of communications) require authorisation by warrants issued by relevant Ministers.

**Relevant secrecy offences**

The United Kingdom has a number of secrecy provisions in the Official Secrets Act 1989. These include a range of offences in sections 1–3 of that Act that generally apply to ‘trusted insiders’ (officers of security, defence, international relations and law enforcement agencies, or other Crown servants or government contractors) who disclose information without authorisation.

There are subsequent disclosure offences in section 5 of that Act by third persons who receive information disclosed without authorisation. These offences require the disclosure to be ‘damaging’ or that the discloser must know or have reasonable cause to believe the disclosure would be ‘damaging’.

As Professor Clive Walker noted in his submission to the inquiry, there is no real equivalent to the SIO scheme or section 35P of the ASIO Act in the United Kingdom, and the closest offence provision in the United Kingdom to section 35P is the disclosure offence in section 39 of the Terrorism Act 2000.

Section 39 of Terrorism Act provides that it is an offence to disclose to another anything that is likely to prejudice the investigation, or interfere with material that is likely to be relevant to the investigation, in circumstances in which a person knows or has reasonable cause to suspect that a constable is conducting or proposes to conduct a terrorism investigation.
It is a defence to an offence against section 39 of the Terrorism Act of if the person did not know and had no reasonable cause to suspect that the disclosure or interference was likely to affect a terrorist investigation or that he had a reasonable excuse for the disclosure or interference.

The offence in section 39 of the Terrorism Act is broader than the offence in section 35P of the ASIO Act, as the section 39 offence is not confined to an SIO but can relate to any terrorism investigation. At the same time, the range of SIOs to which section 35P relates is not limited to terrorism operations and the relevant information need only ‘relate to’ an SIO. As mentioned above, the offence in section 39 of the Terrorism Act is also narrower in that it requires prejudice to, or interference with, a terrorism investigation.

Also of relevance are sections 58 and 58A of the Terrorism Act 2000. Section 58 relevantly provides, broadly, that a person who collects, makes a record of or possesses information of a kind likely to be useful to a person committing or preparing an act of terrorism commits an offence. Section 58A relevantly criminalises eliciting, publishing or communicating information about members of the security services (among others) where the information is by its nature designed to provide practical assistance to a person committing or preparing an act of terrorism. The range of information to which these offences apply seems narrower than that described in section 35P of the ASIO Act, and there are ‘reasonable excuse’ defences to the offences.

Another aspect of the United Kingdom approach to dealing with the media in connection with publications related to national security matters is the ‘DSMA Notice’ system—a voluntary code which operates in relation to certain information and in respect of which the Government and media engage before potentially-relevant publications occur. This system and a now-defunct Australian equivalent system are discussed separately below.

**The Unites States**

**Authorised illegal acts**

In the United States, the Attorney-General’s Guidelines to the FBI Regarding the Use of FBI Confidential Human Sources (signed 13 December 2006) enable the Federal Bureau of Investigations (FBI) to authorise a confidential human source to engage in any activity which would otherwise constitute a criminal violation. The FBI has law enforcement functions and differs from ASIO in this respect.
Before authorising illegal activity, the FBI agent in charge of the matter and the Chief Federal Prosecutor must be satisfied that this activity is necessary to either:

- obtain information essential for the success of an investigation that is not reasonably available without such an activity, or
- prevent death, serious bodily injury or significant damage to property, and
- that the benefits to be obtained from participation in the illegal activity outweigh the risks to the confidential human source.

Certain illegal acts may never be authorised—a confidential human source may not be authorised to participate in any act of violence except in self-defence, or in an act designed to obtain information for the FBI that would be unlawful if conducted by a law enforcement agency (such as breaking and entering and illegal wiretapping).

Authorised illegal acts are not the subject of any statutory legal immunity as such. The guidelines establish a mechanism for notification of relevant prosecuting authorities of a person’s status as an informant and of authorised conduct. The matter is then left to the discretion of those authorities.

**Relevant secrecy offences**

The United States does not appear to have an offence comparable to section 35P of the ASIO Act.

USC title 18, Chapter 37 (the Espionage Act offences) contains various offences including espionage-type offences, including:

- section 793 (gathering, transmitting or losing defense information)
- section 794 (gathering or delivering defense information to aid foreign government), and
- section 798 (disclosure of classified information).

USC title 50, Chapter 44 contains section 3121 (formerly section 421), which deals with ‘Protection of identities of certain United States undercover intelligence officers, agents, informants and sources’. This section creates 3 offences. The first and second offences apply to insiders and the third offence applies to any person. The third offence requires proof of a pattern of activities intended to identify and expose covert agents.
A paper entitled *Intelligence Identities Protection Act* published by the Congressional Research Service in 2013 describes the First Amendment implications of the third of these offences, which were enacted in 1982:

During Congress’s consideration of the measure, much attention was focused on subsection 421(c) and the First Amendment implications if it were employed to prosecute a journalist or anyone else who might publish the identities of covert agents learned from public sources or through other lawful activity. The Senate Judiciary and Conference Committee addressed these concerns at length. Both concluded that the language of the measure would pass constitutional muster.

There are various other offences directed at insiders who contravene their authority, including:

- USC title 18, section 1924 (unauthorised removal and retention of classified documents and material), and
- USC title 50, section 783 (communication of classified information by Government officer or employee).

Another paper entitled *Criminal Prohibitions on the Publication of Classified Defense Information* published by the Congressional Research Service in 2013 makes the following broad comments relevant to this inquiry concerning the current position in the United States:

This report identifies some criminal statutes that may apply to the publication of classified defense information, noting that these have been used almost exclusively to prosecute individuals with access to classified information (and a corresponding obligation to protect it) who make it available to foreign agents, or to foreign agents who obtain classified information unlawfully while present in the United States. While prosecutions appear to be on the rise, leaks of classified information to the press have relatively infrequently been punished as crimes, and we are aware of no case in which a publisher of information obtained through unauthorized disclosure by a government employee has been prosecuted for publishing it.

...  

The Espionage Act on its face applies to the receipt and unauthorized dissemination of national defense information, which has been interpreted broadly to cover closely held government materials related to U.S. military operations, facilities, and personnel. It has been interpreted to cover the activities of foreign nationals overseas, at least when they take an active part in seeking out information. Although cases involving disclosures of classified information to the press have been rare, it seems clear that courts have regarded such disclosures by government employees to
be conduct that enjoys no First Amendment protection, regardless of the motives of
the divulger or the value the release of such information might impart to public
discourse. The Supreme Court has stated, however, that the question remains open
whether the publication of unlawfully obtained information by the media can be
punished consistent with the First Amendment.

Canada

**Authorised illegal acts**

Part 4 of the recently enacted *Anti-terrorism Act, 2015* relevantly amends (among
other Acts) the *Canadian Security Intelligence Service Act* (CSIS Act).

Section 12 of the CSIS Act now provides that if there are reasonable grounds to
believe that a particular activity constitutes a threat to the security of Canada, the
Canadian Security Intelligence Service (CSIS) may take measures (which must be
reasonable and proportional in the circumstances) within or outside Canada to
reduce a threat to the security of Canada.

The CSIS must not take such measures if they will contravene a right or freedom
guaranteed by the *Canadian Charter of Rights and Freedoms* or will be contrary to
other Canadian law, unless authorised to take them by warrant (issued under
section 21.1, by a judge).

Under section 24.1, in certain circumstances, a person who is requested to assist a
person to whom a warrant under section 21.1 is directed, is justified in assisting the
requester in taking the measure.

A press release issued by the Canadian Government in relation to the *Anti-
terrorism Act, 2015* relevantly states:

- The *Anti-terrorism Act, 2015* serves to:
  
  ... 

  3. Provide the Canadian Security Intelligence Service (CSIS) with the ability, under
the authority of a court, to intervene to prevent specific terrorist plots (now in
force)...

This ability appears to involve a ‘disruption’ type function, whereas ASIO’s function
in conducting SIOs remains an intelligence-gathering one. In practice, ASIO’s
conduct of an SIO may lead to disruption activity, albeit that this may need to
involve other agencies and may need to be further authorised. There is no new
secrecy offence related specifically to this new CSIS ability.
The *Criminal Code* of Canada provides some protection for persons administering and enforcing the law. Section 25.1(2) establishes the principle that it is in the public interest to ensure that public officers may effectively carry out their law enforcement duties in accordance with the rule of law and, to that end, expressly recognises in law a justification for public officers and other persons acting at their direction to commit acts or omissions that would otherwise constitute offences. Sections 25.1–25.4 make provision in this respect.

Nothing in section 25.1 of the *Criminal Code* justifies the intentional or criminally negligent causing of death or bodily harm to another person, wilful attempts to obstruct the course of justice or conduct that would violate the sexual integrity of individuals.

These provisions of the *Criminal Code* relate to law enforcement activities and may correspond more closely to the controlled operations scheme in Part IAB of the Australian *Crimes Act 1914* than to the SIO scheme in the ASIO Act.

**Relevant secrecy offences**

The offences under Canadian law most comparable to section 35P of the ASIO Act appear to be sections 13 and 14 of the *Security of Information Act 1985*. These offences apply to a ‘person permanently bound to secrecy’ (a form of insider) who purportedly, or in fact, respectively, communicates or confirms without authority ‘special operational information’ (terms defined in section 8 of the Act).

The term ‘special operational information’ is relevantly defined as information that the Government of Canada is taking measures to safeguard, which reveals, or from which may be inferred (in broad terms):

- the identity of confidential sources
- the nature or content of plans for military operations in respect of potential or present armed conflict
- covert information and intelligence collection methods
- whether certain matters were, are or are intended to be the object of a covert investigation or of covert information or intelligence collection
- the identity of any person who is, has been or is intended to be engaged in covert information or intelligence collection activity
- the means that the Government used, uses or intends to use, or is capable of using, to protect or exploit information or intelligence (including encryption and cryptographic systems and associated vulnerabilities), or
• information or intelligence similar in nature received from foreign governments.

Section 15 of the Act provides that no person shall be guilty of an offence under section 14 or 15 if the person establishes that he or she acted in the public interest, and explains when a person acts in the public interest, namely:

• the person must act for the purpose of disclosing an offence that he or she reasonably believes has been, is being or is about to be committed by a relevant official, and
• the public interest in the disclosure must outweigh the public interest in non-disclosure.

In this context, a court or judge must determine whether the first condition above is satisfied before considering the second condition, and various factors (going broadly to the reasonableness of the disclosure in the circumstances) are specified in relation to any necessary balancing exercise as between the public interests in disclosure and non-disclosure.

**New Zealand**

*Authorised illegal acts*

New Zealand does not appear to have a scheme comparable to the SIO scheme in the *New Zealand Security Intelligence Service Act 1969* (however, that Act does confer certain immunities on persons, giving effect to certain warrants).

*Relevant secrecy offences*

Section 12A of the *New Zealand Security Intelligence Service Act 1969* provides broadly that a current or former officer or employee of the Security Intelligence Service shall not disclose information gained by or conveyed to him in that capacity otherwise than in the strict course of duties or as authorised by the Minister. Contravention of the section is an offence.

Section 13A of the same Act provides broadly that every person who (except with the written consent of the Minister) publishes or broadcasts, or causes or allows to be published or broadcast, the fact that a person is a member of the Service other than the Director or is connected in any way with such a person commits an offence. This offence corresponds quite closely with section 92 of the ASIO Act.
Section 78 of the *Crimes Act 1961* creates an espionage offence and section 78A of that Act creates an offence for the wrongful communication, retention or copying of official information.

**The DSMA-Notice System in the United Kingdom**

The purpose of the DSMA-Notice System is to prevent inadvertent disclosures of information that would compromise United Kingdom military and intelligence operations and methods, or put at risk the safety of those involved in such operations, or lead to attacks that would damage the critical national infrastructure and/or endanger lives.

The DSMA-Notice System in its present form is the product of revisions made to a pre-existing system following a recent review. The website for the DSMA-Notice System ([www.dsma.uk](http://www.dsma.uk)) explains the recent and longer-term history of the system, which commenced in the lead-up to WWI. It also explains various further details of the system and how it operates. The following material is taken from the website (the reference to the MOD is to the Ministry of Defence, the reference to the DPBAC is to the superseded Defence Press, Broadcasting Advisory Committee and the reference to the DA Notice System is to the superseded Defence Advisory Notice System):

> In June 2014, the Permanent Secretary of the MOD sponsored an Independent Review to examine the purpose, utility and effectiveness of the DPBAC and the DA Notice System, from the perspectives of the government, the media and the wider public, in the contemporary context of 24/7 global media, and to make recommendations.

> The Defence and Security Media Advisory (DSMA) Committee oversees a voluntary code which operates between the UK Government departments which have responsibilities for national security and the media. It uses the Defence and Security Media Advisory (DSMA)-Notice System as its vehicle. The objective of the DSMA-Notice System is to prevent inadvertent public disclosure of information that would compromise UK military and intelligence operations and methods, or put at risk the safety of those involved in such operations, or lead to attacks that would damage the critical national infrastructure and/or endanger lives.

**General introduction to DSMA-Notices**

1. Public discussion of the United Kingdom’s defence and counter-terrorist policy and overall strategy does not impose a threat to national security and is welcomed by Government. It is important however that such discussion should not disclose details which could damage national security. The DSMA-Notice System is a means
of providing advice and guidance to the media about defence and counter-terrorist information the publication of which would be damaging to national security. The system is voluntary, it has no legal authority and the final responsibility for deciding whether or not to publish rests solely with the editor or publisher concerned.

2. DSMA-Notices are issued by the Defence and Security Media Advisory Committee (DSMA Committee), an advisory body composed of senior civil servants and editors from national and regional newspapers, periodicals, news agencies, television and radio. It operates on the shared belief that there is a continuing need for a system of guidance and advice such as the DSMA-Notice System, and that a voluntary, advisory basis is best for such a system.

3. When these notices were first published under their new title of Defence Advisory Notices in 1993, they reflected the changed circumstances following the break-up of the Soviet Union and the Warsaw Pact. The 2000 revision has allowed an overall reduction of the scope of the notices while retaining those parts that are appropriate for the current level of threat that involves grave danger to the State and/or individuals. In 2015 the title of the standing Notices was changed to DSMA Notices. The wording, but not the ambit, of the Notices is currently under review, but the existing wording remains in force for the present. Compliance with the DSMA-Notice system does not relieve the editor of responsibilities under the Official Secrets Act.

4. The Secretary DSMA Committee (the DSMA-Notice Secretary) is the servant of the Government and the Press and Broadcasting sides of the Committee. He is available at all times to Government departments and the media to give advice on the system and, after consultation with Government departments as appropriate, to help in assessing the relevance of a DSMA-Notice to particular circumstances. Within this system, all discussions with editors, publishers and programme makers are conducted in confidence.
The 5 standing DSMA-Notices are as follows...

**DSMA-Notice 01**: Military Operations, Plans & Capabilities

**DSMA-Notice 02**: Nuclear & Non-Nuclear Weapons & Equipment

**DSMA-Notice 03**: Ciphers & Secure Communications

**DSMA-Notice 04**: Sensitive Installations & Home Addresses

**DSMA-Notice 05**: United Kingdom Security and Intelligence Services and Special Services

DSMA-Notice 05 compares most closely to the SIO scheme in terms of subject matter and is set out in full below for that reason:

1. Information falling within the following categories is normally regarded as being highly classified. It is requested that such information, unless it has been the subject of an official announcement or has been widely disclosed or discussed, should not be published without first seeking advice:

   (a) specific covert operations, sources and methods of the Security Service, SIS and GCHQ, Defence Intelligence Units, Special Forces and those involved with them, the application of those methods*, including the interception of communications, and their targets; the same applies to those engaged on counterterrorist operations;

   (b) the identities, whereabouts and tasks of people who are or have been employed by these services or engaged on such work, including details of their families and home addresses, and any other information, including photographs, which could assist terrorist or other hostile organisations to identify a target;

   (c) addresses and telephone numbers used by these services, except those now made public.

2. Rationale. Identified staff from the intelligence and security services, others engaged on sensitive counter-terrorist operations, including the Special Forces, and those who are likely targets for attack are at real risk from terrorists. Security and intelligence operations, contacts and techniques are easily compromised, and therefore need to be pursued in conditions of secrecy. Publicity about an operation which is in train finishes it. Publicity given even to an operation which has been completed, whether successfully or not, may well deny the opportunity for further exploitation of a capability, which may be unique against other hostile and illegal activity. The disclosure of identities can prejudice past, present and
future operations. Even inaccurate speculation about the source of information on a given issue can put intelligence operations and, in the worst cases, lives at risk and/or lead to the loss of information which is important in the interests of national security. Material which has been the subject of an official announcement is not covered by this notice.

* even when used by the National Crime Agency (NCA). This is intended purely to protect national security and not to inhibit normal reporting on law enforcement.

**The defunct D-Notice System in Australia**

Australia had a similar system, called the D-Notice System, for many years. Although there still are certain D-Notices technically in existence, the system is now defunct in practice.

The following discussion of the Australian D-Notice System is based on material provided by the Attorney-General’s Department in response to a question (from the INSLM) about the official status of the system.

The D-Notice system was introduced in Australia in 1952. The D-Notice was a Notice issued to the media by the Defence, Press and Broadcasting Committee dealing with specified subjects bearing on defence or national security and requesting editors to voluntarily refrain from publishing certain information about those subjects. As it was voluntary there was no penalty for non-compliance with a request for non-publication.

The D-Notice committee (chaired by the Minister for Defence and comprising representatives of the government and the print and broadcasting media) last met in 1982. Since then the D-Notices have remained unchanged.

There are four D-Notices that technically remain ‘on the books’, although in practice these have fallen into disuse. The D-Notices cover media reports on:

- Capabilities of the Australian Defence Force, including aircraft, ships, weapons and other equipment
- Whereabouts of Mr and Mrs Vladimir Petrov (this has lapsed as both are deceased)
- Signals intelligence and communications security, including the work of the Defence Signals Directorate (now known as the Australian Signals Directorate), and
• The identification of individuals employed by the Australian Secret Intelligence Service (ASIS) or any details of current or projected foreign intelligence activity of ASIS.

The D-Notice system came under scrutiny as part of the Commission of inquiry into ASIS (1994–95, see Appendix L). The Commission recommended that the D-Notice system be reinvigorated and the Government agreed, indicating also an intention to pursue new secondary disclosure offences. However, that intention was not realised before a change of Government in 1996. It seems that the media, from the mid-1990s, essentially decided to opt out of the voluntary system.

In 2010, the then Attorney-General proposed ‘the possibility of developing a more formal mutually agreed arrangement with the media on the handling of sensitive national security and law-enforcement information’.

The then Attorney-General chaired a round-table in April 2011 which provided an opportunity for senior representatives from media organisations and Commonwealth and State government and law enforcement agencies to discuss the continuing need for open and clear communication between media and law enforcement agencies in the context of reporting on matters involving potentially sensitive national security and law-enforcement information. According to the Attorney-General’s Department submissions to this inquiry:

One of the outcomes of the round-table was an agreed set of overarching principles:

• the overriding importance of preventing harm to the public and operational security and law enforcement personnel;
• the preservation of freedom of speech and editorial independence;
• the requirement for the protection of sensitive security and law enforcement information, including in order for security and law enforcement agencies to effectively conduct their operations; and
• the inherent public interest in news relating to security matters.

Nothing has emerged to suggest a different basic approach since the most recent change of Government in 2013.
Abbreviations

AFP  Australian Federal Police
AGD  Attorney-General’s Department
AGO  Australian Geospatial-Intelligence Organisation
AIC  Australian Intelligence Community
ALRC Australian Law Reform Commission
ASD  Australian Signals Directorate
ASIO Australian Security Intelligence Organisation
ASIS Australian Secret Intelligence Service
CBA  Criminal Bar Association-Victoria
CDPP Commonwealth Director of Public Prosecutions
DIO  Defence Intelligence Organisation
ECHR European Convention on Human Rights
ICCPR International Covenant on Civil and Political Rights
IGIS Inspector-General of Intelligence Services
INSLM Independent National Security Legislation Monitor
NCA (former) National Crime Authority
NSA  National Security Agency
ONA  Office of National Assessment
PJC  Parliamentary Joint Committee
PJCIS Parliamentary Joint Committee on Intelligence and Security
RCIS  Royal Commission on Intelligence and Security
SCAG Standing Committee of Attorneys-General
SIO  special intelligence operation