Attorney-General's Department

Joint Submission from AGD and ASIO to the Acting Independent National Security Legislation Monitor Inquiry into section 35P *Australian Security Intelligence Organisation Act 1979* Disclosure offences relating to special intelligence operations

January 2015

Contents

Purpose of this document

The special intelligence operations (SIO) scheme in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) was developed and is administered by the Office of the National Security Legal Adviser (ONSLA) within the Attorney-General's Department (AGD), in close consultation with ASIO. The ONSLA administers the core pieces of intelligence legislation and related casework within the Attorney-General's portfolio responsibilities, primarily the ASIO Act and those parts of the *Intelligence Services Act 2001* administered by the Attorney-General.[1]

AGD and ASIO have prepared this unclassified submission as an aid to the inquiry by the acting Independent National Security Legislation Monitor (INSLM) into the provisions of section 35P of the ASIO Act, which contain offences for the disclosure of information relating to an SIO. The Prime Minister announced on 7 December that he has requested the acting INSLM to consider section 35P as his first priority upon appointment.

This briefing provides an outline of the SIO scheme, with a focus on the disclosure offences in section 35P. It further details the legislative history of the scheme and the particular offence provisions under review, together with a summary of our analysis of potential amendments to section 35P as proposed by some members of the media and other stakeholders or commentators.

AGD and ASIO would be pleased to assist the acting INSLM with further information as necessary, including participating in informal discussions or appearing at any hearings convened under the *Independent National Security Legislation Monitor Act 2010* (INSLM Act).

Overview of the special intelligence operations scheme

Need for a legislative scheme

The SIO scheme was enacted by the *National Security Legislation Amendment Act (No 1) 2014* (NSLA Act), which received royal assent on 2 October and commenced on 30 October 2014. The scheme is established in a new Division 4 of Part III of the ASIO Act.

The SIO scheme was introduced and enacted pursuant to recommendations of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in its 2013 *Report on Potential Reforms to Australia's National Security Legislation*,[2] and subsequently in its 2014 *Advisory Report on the National Security Legislation Amendment Bill (No 1) 2014*.[3] The SIO scheme is designed to ensure that ASIO has the ability to collect useful intelligence in relation to security threats, by obtaining close access to persons or entities of security interest,

1 Commonwealth of Australia, *Administrative Arrangements Order*, 12 December 2013, pp. 4-8.

2 Tabled 24 June 2013. A copy of this report is provided in the volume of materials accompanying this briefing.

3 Tabled 17 September 2014. A copy of this report is provided in the volume of materials accompanying this briefing.

with appropriate legal protections for participants in such intelligence operations.

In particular, the SIO scheme addresses limitations identified in ASIO's intelligence collection capability arising from the potential exposure of participants to legal liability as a result of their participation in certain intelligence operations. The scheme addresses a further limitation in the admissibility of intelligence as evidence in judicial proceedings, such as prosecutions of security offences. Further details of these limitations, and an outline of the SIO scheme, are provided in the subheadings below.

In broad terms, the SIO scheme addresses these limitations by:

- providing for a limited protection from legal liability for participants in certain intelligence operations conducted by ASIO, where the Attorney-General has authorised them in advance, in accordance with the statutory authorisation criteria and other requirements set out in Division 4; and
- applying a targeted modification of the common law rules of evidence, to remove the risk that evidence obtained in the course of and as part of a covert intelligence operation undertaken by ASIO may be excluded on public policy grounds, merely because it was obtained via conduct that would otherwise have constituted a criminal offence.

The SIO scheme is broadly analogous to that of controlled operations undertaken for law enforcement purposes in Part IAB of the *Crimes Act 1914*. However, consistent with ASIO's statutory functions, the SIO scheme is adapted specifically to the purposes of obtaining security intelligence, rather than law enforcement purposes including the collection of admissible evidence in relation to serious offences.[4]

Limitation 1: exposure to legal liability

Prior to the enactment of the SIO scheme, advice from ASIO was that some significant intelligence operations either did not commence or were discontinued because they risked exposing participants to criminal or civil liability in relation to their conduct. ASIO is required to, and does, act lawfully and could not in the absence of such a scheme 'authorise' unlawful conduct as part of an operation even where that conduct may be necessary for the effective performance of ASIO's statutory functions.

For example, in some cases, ASIO may determine that collecting intelligence on a terrorist organisation may be best achieved by a number of ASIO employees or affiliates associating with its members, to enable ASIO to build a detailed understanding of that organisation over a period of time. However, in the absence of an express legislative immunity from legal liability, such actions may contravene various terrorism-related offences in Part 5.3 of the

4 For an analysis of the key differences between the controlled operations and special intelligence operations schemes, see Attorney-General's Department and ASIO, *Joint Submission to the PJCIS inquiry into the National Security Legislation Amendment Bill (No 1) 2014* (copy enclosed in the accompanying volume of materials).

Criminal Code 1995 (Criminal Code). These include offences in relation to membership of,[5] or association with,[6] a terrorist organisation. Other potentially applicable offences include receiving training from,[7] or providing support to,[8] a terrorist organisation.

In the absence of a statutory SIO scheme, participants in a covert intelligence operation would have been reliant upon the exercise of discretion by law enforcement agencies not to refer such matters for prosecution, and the discretion of Commonwealth, State and Territory offices of public prosecutions not to commence prosecutions. ASIO does, and should, at all times, act lawfully. Such discretion failed to provide certainty or any meaningful assurance to participants in ASIO's covert operations as to their legal status and cannot be relied upon in operational planning. Further it does not mitigate ASIO's responsibility to collect intelligence in a lawful manner.

This position was also anomalous to the legal protections applying to participants in authorised controlled operations conducted by law enforcement agencies, which have been subject to a limited immunity from liability under Part IAB of the Crimes Act since 2010.[9]

It was also anomalous to the legal position under section 14 of the *Intelligence Services Act 2001*, which provides that staff members and agents of the intelligence agencies governed by that Act are not liable for acts done in the proper performance of a function of the relevant agency. The immunity in section 14 extends to the actions of agency staff members or agents that are preparatory or ancillary to acts done in the proper performance of the relevant agency's functions.

These limitations on ASIO's intelligence collection capability were acknowledged by the PJCIS in its 2013 *Report on Potential Reforms to Australia's National Security Legislation.* To address them, the PJCIS recommended that the Government consider introducing a comparable scheme for ASIO's intelligence operations to the controlled operations scheme in Part IAB of the Crimes Act, subject to similar sorts of safeguards applying to that scheme.[10]

The (then) National Security Legislation Amendment Bill (No 1) 2014, including the proposed SIO scheme in Schedule 3, was introduced in the Senate on 16 July 2014 to implement the Government's response to this recommendation. The Attorney-General immediately referred the Bill to the PJCIS for inquiry and report.

5 Section 102.3.
6 Section 102.8.
7 Section 102.5.
8 Section 102.7.
9 Inserted by the *Crimes Legislation Amendment (Serious and Organised Crime) Act 2010*.
10 Recommendation 28.

Limitation 2: potential inadmissibility of intelligence in evidence

In the event that any intelligence collected by ASIO as part of a covert operation was lawfully shared with law enforcement authorities, who may have sought to use it in a prosecution, such evidence was susceptible to exclusion in line with the decision in *Ridgeway v the Queen* (1995) 184 CLR 19. In *Ridgeway*, the High Court held that the balance of public interest considerations favoured the exclusion of certain evidence obtained by the AFP as part of a controlled operation, in the prosecution of a drug offence (being the possession of a prohibited import, contrary to section 223B of the *Customs Act 1901*). The relevant evidence was obtained as a result of unlawful conduct by the AFP in the course of that operation – namely, the involvement of AFP officers in facilitating the controlled importation of an illicit drug by an informer, for the purpose of apprehending and prosecuting the accused person, who procured the importation.

The decision in *Ridgeway* is not authority for a general exclusionary rule of all evidence obtained via the involvement of law enforcement officers in unlawful conduct in the course of, and as part of, an authorised covert operation. However, it enables significant latitude in the exercise of judicial discretion to exclude such evidence, having regard to the balance of public policy considerations identified in the circumstances of individual cases.

In *Ridgeway*, the High Court considered the competing public interests in securing the conviction of wrongdoers, and in discouraging unlawful conduct by law enforcement officers. In the facts of the case before it, the majority of the High Court had determinative regard to the nature and degree of the relevant law enforcement officers' unlawful conduct, and the fact that this conduct constituted an element of the offence charged. The High Court further observed that there was no official disapproval of the criminal activity undertaken by the relevant officers. The majority concluded that, on the strength of these considerations, the public interest was best served by excluding the relevant evidence of the drug importation.

The majority held that the appropriate relief in that case was to quash the conviction and order a permanent stay of any future proceedings in relation to the offences charged. Some members of the Court further remarked, in obiter, that legislative intervention was the preferable means of addressing the practical problems concerning the conduct of controlled operations that were evident in the case before it. (As mentioned further below, *Ridgeway* was a catalyst for legislative amendments by a number of jurisdictions from 1995, and ultimately led to the enactment of a national scheme of controlled operations in 2010, following the development of model national legislation.)

While ASIO's role is to gather intelligence in accordance with its statutory functions under section 17 of the ASIO Act, rather than for evidentiary or law enforcement purposes, there are occasions on which intelligence gathered by ASIO may be used in evidence in court to support criminal prosecutions or in civil proceedings. Most of the major counter-terrorism prosecutions conducted to date have made use of intelligence in evidence. With increased interoperability between ASIO and law enforcement agencies on related investigations, the increasing use of ASIO intelligence as evidence is likely.

As noted in the below outline of key provisions in the SIO scheme, Division 4 contains an express provision (in section 35A) to ensure that a court cannot exercise its discretion to exclude intelligence obtained under an SIO form being used in evidence merely because it was obtained in the course of conduct that would have constituted a criminal offence, but for its authorisation as part of an SIO. Importantly, section 35A does not otherwise displace the general rules of evidence, including judicial discretion to exclude evidence on the basis that its probative value is outweighed by its likely prejudice to the interests of a party. Section 35A replicates a corresponding provision in section 15GA of the Crimes Act, which applies an identical rule to controlled operations conducted by law enforcement agencies under Part IAB of that Act.

Outline of key provisions of Division 4 of Part III – authorisation, oversight, reporting

Division 4 of Part III prescribes the requirements for the authorisation, conduct, oversight and reporting on SIOs. Key provisions are summarised below. The disclosure offences in section 35P are outlined separately below.

Authorisation of SIOs (sections 35B-35D)

Applications for SIO authorities

Section 35B provides for the application-based nature of the SIO scheme. It provides that the persons eligible to make an application are the Director-General, a senior position holder (defined in section 3 as a person who holds or is acting in a position in the Organisation that is equivalent to or higher than an SES employee or known as Coordinator), or an ASIO employee (defined in section 3 as a person employed under section 84 or section 90 of the ASIO Act). Applications must generally be in writing, unless the applicant reasonably believes that the delay associated with a written application may be prejudicial to security. In that event, an application may be made orally in person, by telephone or other means of communication. A written record of the application must be made and provided to the Attorney-General as soon as practicable. Applications can only be made, and authorities granted, on a prospective basis. The SIO scheme is not capable of retrospective operation.

SIO authorities

Section 35C provides for the granting of SIO authorities by the Attorney-General, following an application made under section 35B. The Attorney-General must be satisfied that there are reasonable grounds on which to believe that the matters in subsection 35C(2) exist. These matters include:

- that the SIO will assist ASIO in the performance of one or more special intelligence functions, defined in section 3 as ASIO's functions under paragraphs 17(1)(a), (b), (e) or (f) of the ASIO Act;
- the circumstances are such as to justify the conduct of an SIO;
- any unlawful conduct involved in conducting the SIO will be limited to the maximum extent consistent with conducting an effective SIO;

- the SIO will not be conducted in a way that a person is likely to be induced to commit an offence that the person would not have otherwise have intended to commit; and

- any conduct involved in the SIO will not cause death or serious injury to any person; constitute torture; involve the commission of a sexual offence; or result in significant loss of, or serious damage to, property.

The Attorney-General can also grant an SIO subject to conditions, which may impose further limitations, for example on the participants in an operation or the conduct authorised. A further limitation on the conduct capable of being authorised is set out in section 35L, which provides that conduct that requires a warrant under the ASIO Act, or under a warrant or an authorisation under the *Telecommunications (Interception and Access) Act 1979*, cannot be authorised as part of an SIO under Division 4. Rather, the relevant warrants or authorisations must continue to be obtained separately.

Form requirements – SIO authorities

SIO authorities must generally be provided in writing, and can be provided orally (in person, via telephone or other means of communication) if the Attorney-General is satisfied that there are reasonable grounds on which to believe that the delay caused by giving a written authority may be prejudicial to security. A written record must be made within seven days of the granting of an oral authority.

SIO authorities must document how the SIO will assist the Organisation in performing one or more of its special intelligence functions, identify the participants in the SIO (including by assumed name or code name or number), and state a description of the nature of the conduct that these persons may engage in. Authorities must also specify the period of effect of the SIO authority, being a period not exceeding 12 months, and specify any conditions to which the SIO authority is subject. SIOs commence upon the granting of an authority, and cease at the expiry of the period of effect, unless cancelled before this under section 35G, or the period of effect is varied by the Attorney-General under section 35F (up to a maximum total duration of 12 months).

Effect and operation of SIOs (sections 35H-35N)

Sections 35H-35N deal with the effect and operation of SIOs as authorised under section 35C. The key provision is section 35K, which provides for an immunity from criminal and civil liability in respect of otherwise unlawful conduct authorised as part of an SIO. Subsection 35K(1) provides that the limited immunity applies if the participant engages in conduct in the course of, and for the purposes of, the SIO, and in accordance with the SIO authority (which must identify the person as authorised to engage in the relevant conduct). In addition, the 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. Under subsection 35K(2) Attorney-General may make a legislative instrument imposing further requirements that must be met before the limited immunity may apply. No such legislative instruments have been made as at 12 January 2015.

Oversight and reporting (sections 35PA-35Q)

Sections 35PA and 35Q contain the key notification, reporting and oversight-related provisions in relation to SIOs. These include an obligation on the Director-General of Security to notify the Inspector-General of Intelligence and Security (IGIS) if an SIO is authorised under Division 4 as soon as practicable after the authority is granted (section 35PA). In addition, the Director-General must provide six-monthly reports to the Attorney-General and the IGIS on the conduct of SIOs in force. These reports must address the extent to which the SIO has assisted the Organisation in the performance of one or more of its special intelligence functions. They must also specifically disclose whether the conduct of a participant in an SIO has caused death or injury, involved the commission of a sexual offence, or resulted in loss of or damage to property (section 35Q).

These reports are designed to ensure that the Attorney-General has visibility of the conduct of operations once authorised. The notification and reporting requirements to the IGIS are designed to ensure that the IGIS is provided with timely notification of the commencement and conduct of operations, which may inform the IGIS's decisions about the exercise of powers of oversight (including inquiry and inspection) under the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act).

Protection of information relating to a special intelligence operation in legal proceedings

Section 35R provides for a scheme of evidentiary certificates to protect operationally sensitive information in relation to the granting of an SIO authority. The Attorney-General may issue a prima facie evidentiary certificate, setting out such facts as he or she considers relevant with respect to the granting of an SIO authority.

Section 35R is designed to protect operational information forming part of the factual basis upon which the Attorney-General was satisfied that the authorisation criteria in section 35C were met. This may include, for example, details of the operation and its participants, and details of the circumstances which justify the need for the operation (including the particular security threat).

Importantly, the intelligence obtained pursuant to the operation is not capable of being the subject of a certificate, or the question of whether a participant acted in accordance with an authority. The prima facie nature of certificates also provides parties to legal proceedings in which a certificate is tendered with an opportunity to test its limits.

Safeguards applying to the SIO scheme

Considerable attention was given to the incorporation of appropriate safeguards in the design and Parliamentary scrutiny of the SIO scheme. This included a number of enhancements to the provisions of the Bill as introduced to implement recommendations of the PJCIS in its advisory report on the Bill. Notably, these improvements included a model of Ministerial authorisation rather than internal authorisation by the Director-General of Security (as originally proposed in the Bill as introduced and read a first and second time in the Senate).

A further key Parliamentary amendment was made to require ASIO to notify the IGIS when an SIO authorisation is granted, and to include additional matters in its periodic reports to the IGIS under section 35Q (detailing whether the operation caused death, serious injury or property damage, or involved the commission of a sexual offence).

In addition, conduct constituting torture was expressly excluded from SIO authorisations under section 35C and the limited immunity from legal liability in section 35K in response to a request from some members of the Parliament who sought an explicit assurance that such conduct cannot be authorised as part of an SIO (and therefore immune from criminal responsibility). As noted in the Explanatory Memorandum, the Government is of the view that this exclusion is declaratory of the existing legal position, under which ASIO's statutory functions are not capable of authorising such conduct.

The SIO scheme is subject to the independent oversight of the IGIS under the IGIS Act, including the IGIS's powers of inquiry and inspection. In addition, Division 4 may also be subject to inquiry by the INSLM to the extent that it may be characterised as a 'related law' under subparagraph 6(1)(a)(ii) of the INSLM Act. (For example, on the basis that SIOs may be used as part of a suite of legislative measures available in counter-terrorism investigations.)

Outline of disclosure offences in section 35P

As mentioned above, the disclosure offences in section 35P are based on the corresponding disclosure offences in sections 15HK and 15HL of the Crimes Act in relation to controlled operations. Section 35P contains two offences – a basic offence in subsection 35P(1), and an aggravated offence in subsection 35P(2).

The elements of each offence are itemised below. In broad terms, the basic offence in subsection 35P(1) applies to a person who has intentionally communicated information, and is reckless, at the time of making the communication, to the circumstance that the information related to a special intelligence operation.

The aggravated offence in subsection 35P(2) requires further proof that the person made the disclosure intending to cause a specified form of harm, or that the disclosure will have that effect. (The specified forms of harm relate to prejudicing the conduct of an operation, or endangering health or safety of any person.)

Basic offence – subsection 35P(1)

Element analysis

(1) A person commits an offence if:

(a) the person discloses information; and

Physical element: Conduct Reason: Subsection 4.1(2) of the Criminal Code, which provides that conduct includes an action. Fault element: Intention (that is, the person meant to engage in the conduct of disclosing information – as per the definition of intention in subsection 5.2(1) of the Criminal Code). Reason: Subsection 5.6(1) of the Criminal Code, which provides that the fault element of intention applies to a physical element which consists of conduct.

(b) the information relates to a special intelligence operation.

Physical element: Circumstance Reason: Paragraph 4.1(c) of the Criminal Code, which provides that a circumstance is one in which conduct, or a result of conduct occurs. Fault element: Recklessness. (That is, the person was aware of a substantial risk that the information disclosed relates to a special intelligence operation, and unjustifiably in the circumstances known to him or her took the risk of making the disclosure – as per the definition of recklessness in s 5.4(1) of the Criminal Code). Reason: Subsection 5.6(2) of the Criminal Code, which provides that the fault element of recklessness applies to a physical element which consists of a circumstance.

Penalty: imprisonment for five years.

Summary of policy intention – basic offence

In the course of recent Parliamentary scrutiny of the establishing legislation, the Government expressed the view that the offences in section 35P are necessary and appropriate to protect sensitive information about the existence and conduct of SIOs. These operations are necessarily conducted on a covert basis and are intended to remain covert in perpetuity absent any disclosure required by law.

The basic offence is designed to reflect that the very disclosure of the existence and conduct of an SIO creates an unacceptable risk that the operation may be compromised, and that the safety of the participants (and potentially their family or associates) may be jeopardised. Such a risk could be immediate, or could arise over the longer term. The disclosure of such information may also jeopardise other investigations where there is some connection between the two – for example, if there is some relationship between the persons being investigated or an authorised participant, whose identity is disclosed, is known to associate with other persons who are also performing investigative roles.

Once such information is disclosed, there is very limited (or potentially no) 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 persons who act with a

malicious intention since this may further increase the prospects that these risks may eventuate. As such, there is a need for a strong deterrent to the disclosure of information relating to SIOs.

A number of independent reviews of intelligence and secrecy legislation have found that it is appropriate to criminalise the disclosure of intelligence-related information on the basis that harm is inherent or implicit in the very act of disclosure, thereby obviating a need to prove any specific malicious intention on the part of the disclosure, or an adverse outcome of the disclosure. These have included the Hope Royal Commission on Intelligence and Security in its 1976 report on ASIO (affirmed in the 1984 report of the Hope Royal Commission on ASIO) and the Australian Law Reform Commission (ALRC) 2009 *Report on Secrecy Laws and Open Government in Australia*, which specifically examined secrecy offences in respect of the Australian Intelligence Community. The ALRC concluded that secrecy offences in respect of intelligence-related information did not need to include an element requiring proof of harm or intent to cause harm in making a disclosure, on the basis that the harm is implicit.[11]

Summary of policy intention – maximum penalty applying to the basic offence

The basic offence in subsection 35P(1) carries a maximum penalty of five years' imprisonment, which is greater than the two-year maximum penalty applying to the basic offence in section 15HK of the Crimes Act in relation to controlled operations.

A maximum penalty of five years' imprisonment is considered appropriate to reflect the wrongdoing inherent in the reckless disclosure of information relating to an SIO. As mentioned above, information about the existence and conduct of a special intelligence operation is inherently sensitive due to the necessarily covert nature of these operations. The disclosure of such information, by its very nature, places at risk the conduct of the operation to which it relates. This risk arises in respect of both the potential frustration of the effective conduct of an operation (and therefore the ability of ASIO to collect vital intelligence) and in potentially jeopardising the lives and safety of participants.

The proposed maximum penalty further reflects that the person disclosing the information was reckless as to the circumstance of its relationship with a special intelligence operation. That is to say, the person was aware of a substantial risk that the information was so related, but nonetheless, and unjustifiably in the circumstances, took the risk of making the disclosure. A person who was unaware of a substantial risk, or whose conduct is considered by a trier of fact to be justifiable would not be criminally responsible. It is a matter for a sentencing court to determine an appropriate penalty within the maximum, in accordance with general sentencing rules and having regard to the circumstances of individual cases. A person who, for example, disclosed information knowing that it related to a special intelligence operation would reasonably be expected to be subject to a higher penalty than a person who was aware of a substantial risk of this connection.

11 ALRC, *Secrecy Laws and Open Government in Australia,* ALRC Report 112 (2009), p. 289 at [8.65] and recommendation 8-2 at p. 307.

The proposed maximum penalty would also maintain 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 questioning and detention warrants. These offences, which were enacted in the *ASIO Legislation Amendment Act 2006* (Bill of 2006), similarly do not require proof of harm or intention to cause harm in the making of a disclosure, in recognition that such harm is implicit. This approach was found acceptable to the Parliament in 2006.

The Government has expressed a view that a coherent and consistent penalty structure within the ASIO Act is necessary to adequately reflect the harm implicit in the disclosure of information about a covert intelligence activity. (Namely, the significant risk that a covert operation may be compromised.)

Aggravated offence – subsection 35P(2)

Element analysis

(2) A person commits an offence if:

(a) the person discloses information; and

Physical element: Conduct Reason: Subsection 4.1(2) of the Criminal Code, which provides that conduct includes an action. Fault element: Intention. (That is, the person meant to engage in the conduct of disclosing information – as per the definition of intention in subsection 5.2(1) of the Criminal Code.) Reason: Subsection 5.6(1) of the Criminal Code, which provides that the fault element of intention applies to a physical element which consists of conduct.

(b) the information relates to a special intelligence operation; and

Physical element: Circumstance Reason: Paragraph 4.1(c) of the Criminal Code, which provides that a circumstance is one in which conduct, or a result of conduct occurs. Fault element: Recklessness. (That is, the person was aware of a substantial risk that the information disclosed relate to a special intelligence operation, and unjustifiably in the circumstances known to him or her took the risk of making the disclosure – as per the definition of recklessness in subsection 5.4(1) of the Criminal Code.) Reason: Subsection 5.6(2) of the Criminal Code, which provides that the fault element of recklessness applies to a physical element which consists of a circumstance.

(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

Fault element: Intention Reason: Specified in the provision.

(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.

Fault element: Recklessness Reason: Subsection 5.6(1) of the Criminal Code, which provides that the fault element of recklessness applies to a physical element comprising a circumstance.

Penalty: imprisonment for 10 years.

Summary of policy intention – aggravated offence and maximum penalty

The policy intention applying to the aggravated offence is, as noted above, that a disclosure made with a specific malicious intent carries a greater risk of causing harm. Hence, a higher penalty is appropriate to ensure that a sentencing court can impose a penalty reflecting this. The maximum penalty of 10 years' imprisonment is aligned with that applying to the aggravated offence in section 15HL of the Crimes Act.

Exceptions – subsection 35P(3)

The offences in subsections 35P(1) and 35P(2) are subject to a number of exceptions (offence-specific defences) in subsection 35P(3), in addition to the general defences and excuses in Chapter 2 of the Criminal Code. The exceptions in subsection 35P(3) substantially replicate the exceptions to the offences in sections 15HK and 15HL of the Crimes Act, and comprise disclosures made:

- in connection with the administration or execution of the SIO scheme in Division 4;
- for the purpose of any legal proceedings arising out of, or otherwise related to Division 4 (or any report of such proceedings);
- in accordance with any requirement imposed by law;
- in connection with the performance of the functions or duties, or the exercise of powers, of ASIO;
- for the purpose of obtaining legal advice in relation to an SIO;
- to an IGIS official for the purpose of the IGIS exercising powers or performing functions or duties under the IGIS Act; or
- by an IGIS official in connection with the IGIS exercising powers or performing functions or duties under the IGIS Act.

Consistent with subsection 13.3(3) of the Criminal Code, a defendant bears an evidential burden in relation to these exceptions. Consistent with the *Prosecution Policy of the Commonwealth*, the CDPP is required to consider the availability and strength of such exceptions as part of making decisions about whether to commence or continue a prosecution.[12]

12 *Prosecution Policy of the Commonwealth*, updated 9 September 2014, at p.4, paragraph [2.6] (copy provided in the accompanying volume of materials).

These exceptions give effect to a policy position that disclosures of information relating to SIOs are appropriately made via primarily internal means (such as the making of complaints or bringing of matters to the attention of the IGIS, including in accordance with the *Public Interest Disclosure Act 2013*) rather than via indiscriminate, public means.

Geographical jurisdiction – subsections 35P(4) and 35P(5)

Subsection 35P(4) provides that the offences in subsections 35P(1) and 35P(2) are subject to Category D extended geographical jurisdiction under section 15.4 of the *Criminal Code 1995*. This means that a prosecution can be brought in relation to conduct occurring wholly outside Australia. (However, section 16.1 of the Criminal Code requires that the Attorney-General's consent is required to a prosecution brought under Category D jurisdiction, if the person is not an Australian citizen or a body corporate incorporated under an Australian law.)

Subsection 35P(5) is included for the avoidance of doubt because the enactment of the ASIO Act pre-dated the enactment of the general principles of criminal responsibility in Chapter 2 of the Criminal Code (which are now applied to section 35P). Subsection 35P(5) ensures that the express application of Category D jurisdiction to the offences in subsections 35P(1) and (2) does not modify the geographical jurisdiction applying to other offences in the ASIO Act.

Operational and administrative safeguards

Prospective prosecutions of offences against section 35P are subject to three additional administrative safeguards.

Prosecution Policy of the Commonwealth

First, the *Prosecution Policy of the Commonwealth* requires the CDPP to take into consideration the public interest in commencing or continuing a prosecution.[13] As noted in the Explanatory Memorandum to the Bill, it is open to the CDPP to take into account any public interest in a disclosure as part of applying the public interest test.

The prosecution must also consider the availability and sufficiency of admissible evidence in relation to each element of the offence charged, and must be satisfied of its sufficiency to support a conviction.[14] This requires the prosecution to consider the prospects of a jury being satisfied, beyond reasonable doubt, that the person was reckless as to the relationship of the information disclosed to an SIO at the time of making the disclosure. In particular, the prosecution must be satisfied that the unjustifiable nature of the disclosure is capable of proof beyond reasonable doubt (in addition to proof of the person's awareness of a substantial risk that the information related to an SIO). The existence of evidence suggesting reasonable doubt of these requirements is a factor tending against the commencement or continuation of a prosecution.

13 *Prosecution Policy of the Commonwealth*, updated 9 September 2014, at pp.5-6, paragraphs [2.8] – [2.10] (copy provided in the accompanying volume of materials).

14 *Prosecution Policy of the Commonwealth*, updated 9 September 2014, at pp.4-5, paragraphs [2.4] – [2.7] (copy provided in the accompanying volume of materials).

CDPP National Legal Direction

Secondly, on 29 October 2014, the Commonwealth Director of Public Prosecutions (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*. That Direction relevantly requires prosecutors to seek the personal approval of the Director to any proposed prosecutions of offences against section 35P. It also requires prosecutors to consider inviting a prospective defendant to make submission on the public interest, if any, in a disclosure where the prosecutor considers the competing arguments are finely balanced.[15]

Attorney-General's Direction to the CDPP

In addition, on 30 October, the Attorney-General issued a direction to the CDPP under section 8 of the *Director of Public Prosecutions Act 1983*.[16] This direction requires the CDPP to obtain the consent of the Attorney-General to the prosecution of a journalist for certain disclosure offences in security and intelligence legislation, where the facts constituting the alleged offence relate to the work of the person in a professional capacity as a journalist. (The offences covered by the direction are section 35P, the controlled operations disclosure offences in sections 15HK and 15HL of the Crimes Act, and a disclosure offence applying to delayed notification search warrants in section 3ZZHA of the Crimes Act). The CDPP issued an update to its National Legal Direction on 1 December to make reference to the Attorney-General's section 8 direction.

Comparison with disclosure offences in relation to controlled operations

The offences in section 35P are identical to those in sections 15HK and 15HL of the Crimes Act, subject to two exceptions. These are the maximum penalty for the basic offence (as noted above), and exceptions in the Crimes Act for disclosures made to law enforcement oversight bodies (namely, the Ombudsman and the Australian Commissioner for Law Enforcement Integrity, including in relation to integrity testing).[17] The latter exceptions are specific to law enforcement and, accordingly, are not replicated in subsection 35P(3). Instead, they are replaced with an equivalent reference to the IGIS as the relevant oversight body for ASIO.

The AFP has advised that there have been no prosecutions or referrals for prosecution in relation to sections 15HK and 15HL since their enactment in 2010. (Further background on the analogous scheme of controlled operations is provided below.) In second reading debate in the Senate, the Attorney-General indicated that, in the Government's view, this provides assurance that the Crimes Act offences are not operating as an undue limitation on reporting of national security matters, and that section 35P is not likely to operate as such a limitation.

15 A copy is provided in the volume of materials accompanying this briefing.

16 A copy is provided in the volume of materials accompanying this briefing.

17 Subsections 15HK(2A), 15HK(3), 15HL(2A) and 15 HL(3).

Background to the analogous scheme of controlled operations

As mentioned above, the SIO scheme is based broadly on the controlled operations regime for law enforcement agencies in Part IAB of the Crimes Act, with appropriate modifications to reflect the security intelligence, rather than law enforcement, purpose to which the SIO scheme is directed.

In broad terms, the controlled operations scheme enables law enforcement agencies to undertake covert operations, in which law enforcement personnel and other operatives participating in an operation may take an active part in, or otherwise be involved in, the commission of an offence or conduct that may result in a civil liability for the purposes of obtaining evidence that may lead to the prosecution of a person for a serious offence.

The scheme provides participants in authorised operations with a limited protection from legal liability, in respect of actions undertaken in accordance with an authorisation. The scheme also provides that evidence is not to be ruled inadmissible merely because it was obtained as a result of conduct that would, but for its authorisation as part of a controlled operation, constitute a criminal offence.

As noted above, the controlled operations scheme also contains offences in sections 15HK and 15HL for persons who disclose information relating to a controlled operation (on which the offences in section 35P is based). The offences apply to persons who intentionally disclose information, reckless as to whether that information relates to a controlled operation. An aggravated offence applies to persons who make a disclosure intending to prejudice the effective conduct of an operation, or intending to endanger the health or safety of any person. An aggravated offence further applies to a disclosure that will result in either of these outcomes, without requiring specific proof of a person's intention. The controlled operations scheme includes a number of safeguards, including a specific oversight and reporting role for the Commonwealth Ombudsman.

The controlled operations scheme has been in existence in its present form since 2010, following an agreement of Commonwealth, State and Territory leaders in 2009 to establish a national framework for the regulation of these operations. The 2009 agreement had its origins in a national consultation and policy development process that commenced in 2003, under the auspices of the former Standing Committee on Attorneys-General (SCAG) and a First Ministers' forum, the Leaders' Summit on Terrorism and Multijurisdictional Crime.

The model controlled operations provisions developed by the former SCAG, which were endorsed by First Ministers in 2003, contained model disclosure offence provisions identical to those which are now contained in sections 15HK and 15HL of the Crimes Act. As mentioned above, these offence provisions are replicated in section 35P of the ASIO Act (subject to the adoption of a different penalty structure in the ASIO Act, for the reasons set out above).

Prior to the enactment of the national controlled operations scheme in 2010, the use of such operations was regulated in a fragmented manner under individual State and Territory

legislation and administrative arrangements. While controlled operations were utilised by law enforcement agencies prior to 1995, operatives were not subject to any legislative protection from legal liability in respect of authorised conduct. They were reliant upon prosecutorial discretion, together with judicial discretion to admit evidence obtained in the course of a controlled operation in the course of a prosecution or another form of legal proceedings. The impetus for legislative reform was principally the decision of the High Court in *Ridgeway v the Queen* (discussed above), together with an identified need to better facilitate cross-border and multi-agency operations via a nationally coherent and consistent legislative framework.

Legislative history of section 35P

Parliamentary Joint Committee on Intelligence and Security 2012-2013 inquiry

In 2012, the former Government referred a range of potential reforms to national security legislation to the PJCIS for inquiry and report. These possible reforms were identified in the course of consultations with security and intelligence agencies, including legislative limitations identified through recent operational experience.

The former Government identified a range of measures it intended to pursue, and a range of others on which it sought the PJCIS's views about their viability. This included a series of proposed amendments to the ASIO Act and the *Intelligence Services Act 2001* to modernise the legislative framework governing the Australian Intelligence Community and ensure its capacity to respond effectively to current, emerging and future security threats (including in light of rapid technological developments and their use in counter-intelligence measures by persons of security concern). The former Government identified a regime of SIOs as a measure it intended to pursue, for the reasons identified above, and sought the views of the PJCIS on this proposal.

The PJCIS tabled its report on 24 June 2013, relevantly recommending (in Chapter 4) that the Government proceed with or give further consideration to the majority of the proposed reforms to intelligence legislation. This included recommendation 28, "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*". The Committee did not document any specific analysis of, or recommendations in relation to, disclosure offences in relation to the proposed SIO scheme. However, to the extent it recommended that the scheme adopt "similar safeguards" to those in the Crimes Act, its conclusions were interpreted as a mandate to include such offences in the SIO scheme, since disclosure offences are designed to safeguard sensitive operational information against compromise (and also contain a number of safeguards to ensure that the offences are proportionate to the legitimate objective to which they are directed).

The Government introduced the *National Security Legislation Amendment Bill (No 1) 2014* in the Senate on 16 July 2014, implementing its response to the recommendations in Chapter 4 of the PJCIS's 2013 report. Schedule 3 to the Bill included the proposed SIO scheme in

Division 4 of Part III of the ASIO Act. Upon the introduction of the Bill, the Attorney-General referred it to the PJCIS for inquiry and report by 17 September 2014. AGD and ASIO engaged extensively with the PJCIS, including appearances at public and private hearings and the provision of detailed written submissions.[18] SIOs, including the offences in section 35P, were a focal point of the Committee's inquiry.

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.[19] 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

18 Copies of these submissions are in the volume of materials accompanying this briefing

19 Other key areas of inquiry in relation to the SIO scheme included differences with the controlled operations scheme and the reasons for these, and the appropriate model of authorisation (internal or external). These are summarised in the PJCIS report of 17 September 2014 (copy provided in the volume of this briefing).

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.

AGD and ASIO gave extensive evidence to the PJCIS about the legal and policy issues arising in relation to these proposals (detailed subsequently in this background paper).

In addition to the issues identified by media and other stakeholders, the IGIS also raised concern that the offences as introduced did not contain a specific exception for disclosures made to the IGIS or IGIS staff members for the purpose of the performance of functions or duties, or the exercise of powers under the IGIS Act. (Such an exemption was not included in the Bill as introduced and read a first and second time in the Senate because the *Public Interest Disclosure Act 2013* and the provisions of the IGIS Act were considered to override the offence provisions. However, the IGIS recommended an express exception to avoid any perceived deterrent effect in relation to persons considering making disclosures of suspected wrongdoing to the IGIS.)

Parliamentary Joint Committee on Intelligence and Security 2014 inquiry

The PJCIS gave detailed consideration to section 35P in the course of its inquiry into the Bill. The Committee made the following comments in its Advisory Report on the Bill:

> 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 *Public Interest Disclosure Act 2013*, 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.[20]

The Committee made the following recommendations in relation to section 35P:

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

20 PJCIS *Advisory Report on the National Security Legislation Amendment Bill (No 1) 2014*, 17 September 2014, pp. 61-63.

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.

The Government supported all of these recommendations,[21] and implemented them by moving Parliamentary amendments to the Bill in the Senate, and issuing a replacement Explanatory Memorandum.

Parliamentary debate in relation to section 35P, including cross-bench amendments

Section 35P attracted considerable attention in the course of the Parliamentary debate of the Bill. As noted above, several members of the cross-bench unsuccessfully moved amendments in the Senate, including:

- a specific whistleblowing exception for public disclosures made in the public interest;
- to repeal the basic offence in subsection 35P(1); and
- to require sentencing courts to take into account the public interest (if any) in disclosures made by a person convicted of an offence against subsection 35P(1) or subsection 35P(2)

The Government and the Opposition voted against these proposed amendments.[22] Detailed analysis of them (and other amendments proposed by various stakeholders) is set out below (under the heading "Comments on stakeholders' proposed amendments to section 35P").

Post-enactment developments in relation to section 35P

CDPP National Legal Direction and the Attorney-General's section 8 direction

As mentioned above, the CDPP issued a National Legal Direction in relation to the prosecution of offences against section 35P on 29 October (updated on 1 December). The Attorney-General issued a direction to the CDPP on 30 October, requiring the CDPP to obtain the Attorney-General's consent to the commencement of a prosecution of a journalist for an offence against section 35P. The power to issue directions to the CDPP is exercised rarely, having regard to the independence of the Office of the CDPP.

21 Government response to the PJCIS Advisory Report on the National Security Legislation Amendment Bill (No 1) 2014, 19 September 2014 (copy provided in the volume of materials accompanying this briefing).

22 See *Senate Hansard*, 25 September 2014 (copy provided in the volume of materials accompanying this briefing).

Delayed reporting by the Parliamentary Joint Committee on Human Rights on the Bill

In addition, the Parliamentary Joint Committee on Human Rights (PJCHR) examined and concluded its consideration on the Bill subsequent to its enactment.

This included an examination of section 35P, and in particular its compatibility with the right to freedom of expression in Article 19(2) of the International Covenant on Civil and Political Rights (ICCPR). The PJCHR opined that section 35P is, in its view, 'incompatible' with Article 19(2). The Committee stated that its reasoning for adopting this opinion was that the Statement of Compatibility with Human Rights in the Explanatory Memorandum accompanying the Bill did not provide, in its view, enough information for the Committee to identify a legitimate objective to which the offence was directed, and to establish that any limitations on the right to freedom of expression imposed by the offences was necessary for, and proportionate to, the achievement of that objective.[23]

With respect, the Department is of the view that this reasoning is unsound as a matter of law, since a perceived absence of information means that there is no evidence base or body of legal analysis to substantiate any conclusion. 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.[24]

The Department (ONSLA, in consultation with the Office of International Law) is able to provide further information to the INSLM about the Government's position on the human rights compatibility of the SIO scheme, including section 35P, if required.

Government engagement with media stakeholders in relation to section 35P

The Attorney-General has also engaged extensively with media stakeholders in relation to section 35P, subsequent to its enactment on 2 October and commencement on 30 October. This has included the publication of an opinion article in *The Australian* on 14 October, an appearance on the ABC's *Question and Answer* program on 3 November, and responses to numerous media requests for comment, including ABC Media Watch (with the response broadcast on 6 October).

---

23 Parliamentary Joint Committee on Human Rights, Sixteenth Report of the 44th Parliament, pp. 55-57. A copy of this report is provided in the volume of materials accompanying this briefing.

24 This correspondence was published in the Committee's Sixteenth Report (referenced above).

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. Copies of these submissions, together with the Committees' reports, are provided in the volume of extrinsic materials accompanying this briefing.

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 re-consider 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.

Possible ways forward in relation to section 35P

Suggested option – retain the status quo, subject to ongoing INSLM review

We are of the view that there is a satisfactory policy justification for retaining the offences in subsection 35P in their present form, subject to one suggested amendment as detailed below.

In particular, we are of the view that the offences give effect to the legitimate objective of protecting sensitive information about the existence and conduct of SIOs, and preventing the risk of harm that arises from the mere fact of disclosure – irrespective of the discloser's intentions or position. This policy position is consistent with a body of opinion arising from independent reviews, including the Hope Royal Commission and, more recently, the Australian Law Reform Commission in its review of Commonwealth secrecy laws. It is also consistent with precedent in the controlled operations disclosure offences, which were enacted following national agreement and have not resulted in any prosecutions to date (including of journalists).

To the extent that the SIO regime may be utilised in counter-terrorism operations, it falls within the statutory remit of the INSLM, pursuant to subparagraph 6(1)(a)(ii) of the INSLM Act. The INSLM Act therefore provides for an avenue of ongoing, independent monitoring and review of the operation, effectiveness and implications of section 35P. Such a review mechanism will assist in identifying whether the offences are operating as intended. In the event any concerns are substantiated through operational experience, the oversight and analysis of the INSLM may also provide a credible evidence base for reform.

Suggested minor amendment – statutory prosecutorial consent requirement

Given that prosecutorial consent requirements are generally incorporated in the relevant offence provisions rather than by way of an executive direction, we consider there would be benefit in inserting a general prosecutorial consent requirement in section 35P.

Having the requirement for prosecutorial consent apply in respect of the provision as a whole rather than just in relation to the prosecution of journalists could also alleviate the difficulty identified by the PJCIS in identifying a person as a journalist for the purpose of the prosecutorial consent requirement, and could remove any potential (actual or perceived) for arbitrariness in this regard.

Possible consideration of targeted amendments to the physical elements

In the event that the INSLM forms a view that amendments are required to the elements of the offences in section 35P to modify their application in relation to public disclosures of information relating to an SIO, consideration could be given to adopting some of the elements of the offences in section 34ZS of the ASIO Act. (These offences apply to persons who make disclosures in relation to ASIO's questioning warrants or questioning and detention warrants issued under Division 3 of Part III of the ASIO Act.)

While this section identifies possible areas in which alignment could be considered between section 35P and section 34ZS, AGD does not consider that such alignment is appropriate (although such amendments would, on our assessment, present fewer difficulties than other suggested amendments examined in the previous section of this paper). The differences in the physical elements of the offences in sections 35P and 34ZS reflect fundamental differences in the nature of special intelligence operations, and questioning and questioning and detention warrant operations.

In particular, the offences in section 34ZS of the ASIO Act are directed to deterring and penalising the harm that may be sustained in relation to a single warrant operation which is of limited duration (that is, the questioning under warrant of an individual person over a period of hours). In contrast, SIOs are undertaken on a much larger scale and run over a considerably longer period of time (being 12 months, subject to multiple renewals). This is consistent with their objective to obtain detailed information on targets over a sustained period of time, via covert means, as distinct from the objective of questioning warrants and questioning and detention warrants, which is to obtain intelligence in relation to a terrorism offence (including intelligence that can be used to prevent the commission of a terrorist act). In the event that alignment was pursued, appropriate adjustments would need to be made to the specific provisions applied in section 34ZS, as they are not suitable to be replicated exactly in section 35P given the different nature of operations under Divisions 3 and 4 of Part III.

Possible limitations on the type of information subject to the disclosure offences.

The offences in section 35P apply to the disclosure of information that relates to an SIO, where the disclosure is reckless as to that relationship between the information and the SIO. The precise type of relationship between the information and the SIO is not prescribed or otherwise limited. In contrast, section 34ZS applies to information that does either or both of the following (while the warrant is in force):

- indicates the fact that the warrant has been issued, or a fact relating to the content of a warrant, or to the questioning or detention of a person in connection with the warrant; and/or
- is operational information.

In the event that the information is operational information that does not additionally indicate the facts in the first point above, the operational information must have come into the knowledge or possession of the discloser as a direct or indirect result of the issue of the warrant, or the doing of anything authorised by the warrant, or under directions given in connection with the warrant, or by another provision of Division 3 of Part III in connection with the warrant.[25]

In the case of disclosures of such information made after the period of effect of the warrant has expired, but within two years of the expiry of that period, a disclosure offence applies to information that is operational information, which has come into the possession of the person

25 Subsection 34ZS(1).

as a direct or indirect result of the circumstances mentioned in the above paragraph.[26]

As these physical elements of the offences in section 34ZS are circumstances in which conduct occurs (that conduct being the disclosure of information) they attract the fault element of recklessness.[27] This is so unless the defendant is the subject of the warrant or a lawyer representing such a person, in which case strict liability applies by reason of paragraphs 34ZS(3)(a) and (b).

Consideration could potentially be given to applying an analogous limitation to the elements of subsections 35P(1) and 35P(2), at least to the extent that the information disclosed must either indicate the existence of an SIO, or the content of an SIO authority (in terms of disclosing authorised conduct and participants, targets and other information about the satisfaction of the authorisation criteria), or the conduct of an SIO in accordance with an authority.

However, the risk associated with this greater degree of specificity in the physical elements of the offences in section 35P is that it increases the degree of difficulty in establishing the attendant fault elements. (That is, the prosecution must prove a person was reckless as to the particular type of relationship between the information disclosed and the SIO.) The more narrowly or specifically that circumstance is prescribed in the physical elements of the offence, the greater the possibility for reasonable doubt to exist, especially in relation to the attendant fault elements. This may produce the unintended consequence that conduct that should properly be regarded as culpable (due to the risk it presents of operational compromise or harm to participants) may go unpunished on the basis of a technicality as to the particular nature of the relationship between the information disclosed and the SIO.

The risk of harm in relation to the disclosure of the existence of an SIO (or any other information that may compromise its effective conduct) is arguably greater than that which may arise in relation to questioning warrants and questioning and detention warrants. As mentioned above, the latter types of warrants authorise a single activity (namely coercive questioning of an individual). Although the dissemination of information relating to questioning warrants and questioning and detention warrants needs to be contained to ensure their effectiveness, unlike an SIO they are not a covert means of investigation as the person being questioned is aware that he or she, or persons connected with him or her, are of security interest to ASIO. SIOs are undertaken on a much larger scale and run over a considerably longer period of time. They must remain covert, on an indefinite basis, to their targets and the wider community.

We strongly recommend that, if such an option is considered the course of the INSLM's review, its potential operational impacts be explored in detail with ASIO, and its practical enforcement implications examined with the AFP and the CDPP.

---

26 Subsection 34ZS(2).

27 Subsection 34ZS(3).

Possible time limit on non-disclosure periods

As mentioned above, the disclosure offences in section 34ZS apply either to disclosures made while a questioning or questioning and detention warrant is on foot, or disclosures made within two years of the expiry of their period of effect.

Consideration could be given to limiting the offences in section 35P to disclosures made within a certain period of time of a special intelligence operation commencing (or concluding). However, we do not consider that such a time limit is appropriate because it could have significant, detrimental consequences in relation to SIOs that may not arise in relation to questioning warrants and questioning and detention warrants. If such a time limit were to be considered, we are of the view that, for the reasons set out below, the period would need to be in the order of several years (an indicative period may be a decade or decades). We strongly recommend that ASIO is consulted in relation to any possible time limit, to ensure that it is consistent with the nature of special intelligence operations, which are directed to collecting intelligence on an entity or matter of security concern over a sustained period of time.

The key difference between special intelligence operations (to which the disclosure offences in section 35P apply) and questioning and questioning and detention warrants (to which the disclosure offence in section 34ZS applies) is questioning and questioning and detention warrants have a far more limited period of effect than SIOs. The maximum period of effect for questioning and questioning and detention warrants is 28 days, with the maximum duration for questioning under a warrant being 24 hours. A person may only be detained under a questioning and detention warrant for a maximum of 168 hours, and questioned for a maximum of 24 hours within that time.

In contrast, an SIO does not necessarily involve a single person as its target, and involves a range of activities. Its maximum period of effect is 12 months, with the ability to apply for an unlimited number of new authorisations upon expiry, provided that the Attorney-General is satisfied the authorisation criteria are met on each occasion a new authorisation is sought. SIOs are intended to operate over a much longer period of time, and are intended to remain covert to their targets and to the wider community indefinitely (unlike questioning and questioning and detention warrants which must necessarily be disclosed to the person being questioned who may be the target of the investigation, their legal representative and potentially other persons, where such disclosure is authorised in accordance with Division 3 of Part III).

Given the broader scope of an SIO than a single questioning or questioning and detention warrant, there is a realistic possibility that the disclosure of information relating to an SIO may produce a greater risk of harm to the integrity of the operation and the safety of its participants (and their families and associates). For the above reasons, this risk of harm may also be more severe in its impact if it were to eventuate, and more difficult (if not impossible) to mitigate.

Further, a fixed time period may be more readily adaptable to the disclosure offences in section 34ZS because questioning and questioning and detention warrants are not covert in that their existence must necessarily be disclosed to the person who is subject to a warrant and others in accordance with the requirements of Division 3. Hence, any fault elements applying to a time period specified in the elements of the offences in section 34ZS are, arguably, more amenable to proof to the criminal standard. In contrast, the commencement and cessation dates of an SIO are less likely to be known, and therefore less amenable to proof by the prosecution, because they are not disclosed to any person outside ASIO (other than the Attorney-General and the IGIS). The inclusion of a fixed-time period in section 35P may therefore set an unattainable bar for prosecutions, which could serve to frustrate the legitimate protective and deterrence-related objectives to which the offences are directed.

A further potential difficulty in specifying a fixed-time period is that the timeframes for SIOs may differ according to the particular security threat to which they are directed (noting the breadth of the matters covered by the term 'security' as defined in section 3 of the ASIO Act). Some types of operations may be much longer than others, or there may be a related, ongoing security investigation which would be compromised by the disclosure of information relating to the SIO even though the SIO aspect had concluded.

As noted above, in the event that a fixed time period is considered in relation to the offences in section 35P, we emphasise the importance of ensuring that any such period accurately reflects the longer-term nature of SIOs and that the operational impacts of any potential fixed time period are explored thoroughly with ASIO.

Given the different nature of questioning and questioning and detention warrants, replicating the time period in section 34ZS of two years after the period of effect of a warrant would not be appropriate in relation to section 35P. (An indicative period may be in the range of several years, potentially a decade or decades). In addition, we consider that the disclosure of information from which the identity of a participant may reasonably be inferred should be excluded from any fixed time period. This is due to the ongoing risks to a participant's safety, including to a participants family or associates, which may arise should their participation be made known. As noted above, this risk does not necessarily abate with the passage of time after the conclusion of an operation, and cannot generally be effectively contained or removed once the identity of a participant is disclosed.

Schedule of attachments (copies provided in accompanying volumes)

Legislation and extrinsic materials

(1) Copy of the provisions of Division 4 of Part III of the *Australian Security Intelligence Organisation Act 1979* (special intelligence operations).

(2) Revised Explanatory Memorandum to the National Security Legislation Amendment Bill (No 1) 2014.

Parliamentary scrutiny of section 35P

(3) Three submissions of the Attorney-General's Department to the Parliamentary Joint Committee on Intelligence and Security inquiry into the National Security Legislation Amendment Bill (No 1) 2014 (August-September 2014) and responses to matters taken on notice at the Public Hearing (August 2014).

(4) Two submissions of the Attorney-General to the Senate Scrutiny of Bills Committee in relation to the National Security Legislation Amendment Bill (No 1) 2014 (August-September 2014).

(5) Parliamentary Joint Committee on Intelligence and Security, *Report on Potential Reforms to Australia's National Security Legislation* (June 2013).

(6) Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the National Security Legislation Amendment Bill (No 1) 2014* (September 2014)

(7) Government Response to the Parliamentary Joint Committee on Intelligence and Security *Advisory Report on the National Security Legislation Amendment Bill (No 1) 2014* (September 2014).

(8) Senate Scrutiny of Bills Committee, Alert Digest No 11 of 2014; and Report No 13 of 2014.

(9) Parliamentary Joint Committee on Human Rights, 16th Report of the 44th Parliament (November 2014).

(10) Senate Hansard, 24 and 25 September 2014 (debate and consideration in committee of the National Security Legislation Amendment Bill (No 1) 2014).

(11) Copies of proposed amendments to section 35P circulated by the Australian Greens, the Liberal Democratic Party and independent Senator Nick Xenophon (24-25 September 2014).

Prosecutorial guidance materials

(12) Prosecution Policy of the Commonwealth (updated 9 September 2014).

(13) CDPP National Legal Direction (updated 1 December 2014).

(14) Attorney-General's direction to the CDPP (30 October 2014).

Other background materials

(15) Attorney-General, Senator the Hon George Brandis QC, opinion article, 'ASIO powers are no threat to journalists', *The Australian*, 14 October 2014, p. 12.

(16) *Ridgeway v the Queen* (1995) 184 CLR 19.