PARLIAMENT OF AUSTRALIA
DEPARTMENT OF PARLIAMENTARY SERVICES

PARLIAMENTARY LIBRARY
INFORMATION ANALYSIS ADVICE

QUICK GUIDE

RESEARCH PAPER SERIES, 2014–15 23 OCTOBER 2014

Offences for disclosing information about covert operations: a quick guide

Cat Barker
Foreign Affairs, Defence and Security Section

The offences for unauthorised disclosure of information about a 'special intelligence operation' were one of the most controversial aspects of the National Security Legislation Amendment Bill (No. 1) 2014 (NSLA Bill). The Bill was passed by both Houses of Parliament (with some amendments, including to the offences) and became an Act on 2 October 2014. Debate about the offences was re-ignited when Australian Labor Party front-bencher Anthony Albanese commented on them in an interview on 12 October 2014, in which he suggested they go too far and should be monitored closely. The debate remains relevant in the context of a similar offence relating to delayed notification search warrants proposed in the Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014, which is currently before the Senate.

These offences are different to longstanding secrecy offences such as the offence in section 70 of the *Crimes Act 1914*, which criminalises unauthorised disclosure of official information by someone who is or was a Commonwealth officer. They apply more broadly to any person who discloses particular information, raising concerns that they may inappropriately capture legitimate reporting.

This Quick Guide provides a brief factual overview of the offences, how they operate and the extent to which they apply to public interest disclosures.

Special intelligence operations

As outlined in the Parliamentary Library's Bills Digest, a new Division of the *Australian Security Intelligence Organisation Act 1979* (*ASIO Act*) will establish a 'special intelligence operation' (SIO) scheme under which Australian Security Intelligence Organisation (ASIO) officers and affiliates will be protected from criminal and civil liability for certain conduct engaged in for the purpose of an SIO. Enactment of an SIO scheme modelled on the controlled operations scheme used by law enforcement agencies for undercover operations implements a recommendation in the Independent National Security Legislation Monitor's *Annual report 2014*.

Similar to the controlled operations scheme, the SIO scheme is intended to apply to circumstances where officers would need to engage in conduct that would otherwise constitute an offence in order to maintain their cover. The Attorney-General gave the example of an ASIO officer who had penetrated a terrorist cell being involved in conversations about planning a terrorist attack.

Section 35P of the *ASIO Act* sets out two offences for unauthorised disclosure of information relating to SIOs, in order to 'protect persons participating in an SIO and to ensure the integrity of operations'. The offences are modelled on offences for disclosures relating to controlled operations (but contain some differences):

> (1) A person commits an offence if:
> (a) the person discloses information; and

ISSN 2203-5249

(b) the information relates to a special intelligence operation.
Penalty: Imprisonment for 5 years.

…

(2) A person commits an offence if:
(a) the person discloses information; and
(b) the information relates to a special intelligence operation; and
(c) either:
(i) the person intends to endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation; or
(ii) the disclosure of the information will endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation.
Penalty: Imprisonment for 10 years.

Application of the Criminal Code

The scope of the offences in new section 35P of the *ASIO Act* is affected by the application of the *Criminal Code Act 1995*, specifically Part 2.2, concerning the elements of Commonwealth offences. Broadly, Commonwealth offences are made up of physical elements (which may be **conduct**, a **result** (of conduct) or a **circumstance** (in which conduct or a result of conduct occurs)) and fault elements (which may be **intention**, **knowledge**, **recklessness** or **negligence** or something else). Section 5.6 provides that if an offence does not specify the fault element that applies to a physical element (which is the case for the offences above, except for subparagraph 35P(2)(c)(i), where intention is explicitly applied) then:

- if the physical element is conduct, the fault element of intention applies and
- if the physical element is a circumstance or result, the fault element of recklessness applies.

Division 5 of Part 2.2 of the *Criminal Code* sets out what must be proven to establish different fault elements. Of relevance to the offences in section 35P of the *ASIO Act*:

- 'a person has intention with respect to conduct if he or she means to engage in that conduct'
- 'a person has intention with respect to a circumstance if he or she believes that it exists or will exist' and
- a person is reckless with respect to a circumstance if:
  - 'he or she is aware of a substantial risk that the circumstance exists or will exist' **and**
  - 'having regard to the circumstances known to him or her, it is unjustifiable to take the risk'

It also provides that 'the question whether taking a risk is unjustifiable is one of fact'.

To establish an offence, the prosecution must prove all of the physical and fault elements to the criminal standard of 'beyond reasonable doubt' (sections 13.1 and 13.2 of the *Criminal Code*).

Proving the offences

Accordingly, to establish an offence against new subsection 35P(1) of the *ASIO Act* (punishable by up to five years imprisonment), the prosecution would need to prove beyond reasonable doubt that:

- a person intentionally disclosed information **and**
- the person was aware of a substantial risk that the information related to an SIO, and having regard to the circumstances known to him or her, it was unjustifiable to take the risk.

To establish an offence against subsection 35P(2) (punishable by up to ten years imprisonment), the prosecution would need to prove beyond reasonable doubt the matters above, **and** that:

- the person:
  - intended to endanger the health or safety of any person or prejudice the effective conduct of an SIO **or**
  - was aware of a substantial risk that the disclosure would endanger the health or safety of any person or prejudice the effective conduct of an SIO, and having regard to the circumstances known to him or her, it was unjustifiable to take the risk.

Concerns raised by media organisations that a person could be found guilty of one of these offences for disclosing information that he or she had 'no idea', or was 'not aware', related to an SIO are therefore misplaced. Further, the aggravated offence in subsection 35P(2) would only apply where a person either intended, or was reckless as to whether, his or her disclosure of information relating to an SIO would endanger the health or safety of a person or prejudice the effective conduct of an SIO. It is therefore of very limited relevance to public interest disclosures.

However, there may be instances where a person knows or is aware of a substantial risk that information relates to an SIO, but where he or she believes that there is considerable public interest in making the disclosure—for example, in reporting on misconduct or abuse of powers. This issue of the application of the offence in subsection 35P(1) to such circumstances is taken up below.

Public interest disclosures

A further piece of legislation must be taken into account in determining the scope of the offences for unauthorised disclosures relating to SIOs—the *Public Interest Disclosure Act 2013* (*PID Act*). The *PID Act* provides public sector employees with protection from civil, criminal and administrative liability for making a 'public interest disclosure' in accordance with the Act, in order to 'encourage public officials to report suspected wrongdoing in the Australian public sector'. Under section 29 of the *PID Act*, types of 'disclosable conduct' include, for example, conduct that contravenes an Australian law, involves corruption or abuse of public office, is an abuse of trust, or constitutes maladministration.

However, the protections available under the *PID Act* are limited for employees of intelligence agencies, including ASIO. Disclosures containing 'intelligence information' (defined in section 41) may only be made internally or to the Inspector-General of Intelligence and Security (IGIS). Disclosures not containing intelligence information may be made to other agencies, bodies and individuals in certain circumstances. Under subparagraph 41(1)(b)(iii), intelligence information includes information that is about, or might reveal 'operations that have been, are being, or are proposed to be, undertaken by an intelligence agency'. For a good explanation of the very restricted application of the *PID Act* to intelligence agencies in general and in the context of these offences, see Professor A.J. Brown's submission to a committee inquiry into the NSLA Bill.

Application of the offences to whistleblowers and others, including journalists

Under the *PID Act*, an ASIO officer would be protected from civil, criminal and administrative liability for making a public interest disclosure in relation to an SIO either internally or to the IGIS if it was made in accordance with that Act. The officer would not be protected under the *PID Act* for a disclosure made to anyone else, including to a journalist.

Subsection 35P(3) sets out several exceptions to the disclosure offences, for example, where the disclosure is in accordance with a legal requirement or made to the IGIS for the purpose of the IGIS's performance of powers or functions. It does not provide a public interest exception for persons not covered by the *PID Act*, such as journalists. Where a person knows or is aware of a substantial risk that information relates to an SIO, but believes there is considerable public interest in making the disclosure, he or she is placed in the position of either not making the disclosure, despite the public interest in doing so, or making the disclosure in the hope that the Commonwealth Director of Public Prosecutions (CDPP) would decide not to prosecute on public interest grounds.

The *Prosecution Policy of the Commonwealth* sets out a two-stage test that must be satisfied before the CDPP commences a prosecution:

- there must be a reasonable prospect of a conviction being secured (paragraphs 2.5–2.7) and
- the prosecution must be in the public interest (paragraphs 2.8–2.10).

A legislated exception to the SIO offences would provide clearer protection for public interest disclosures.

Delayed notification search warrants

As outlined in the Parliamentary Library's Bills Digest, the Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014 proposes new Part IAAA be inserted into the *Crimes Act* to establish a delayed notification search warrant (DNSW) scheme for terrorism offences that carry a maximum penalty of at least seven years imprisonment. The scheme would allow the Australian Federal Police (AFP) to conduct searches covertly, but require the owner or occupier of the premises to be notified and provided information about the search at a later date.

Under proposed subsection 3ZZHA(1), a person would commit an offence if:

- the person discloses information (to which the fault element of intention would apply) and
- the information relates to an application for, or the execution of, a DNSW; a report of an executing officer to the Commissioner about the DNSW; or a notice to the occupier of the warrant premises or adjoining premises (to which the fault element of recklessness would apply).

The maximum penalty would be imprisonment for two years. As with the offences for disclosure of information about SIOs, several exceptions would be provided, but there would be no exception for public interest disclosures. Other potential issues in relation to the proposed offence are outlined in the Bills Digest.

The *PID Act* applies more broadly to AFP officers than to ASIO officers. As well as making a public interest disclosure internally and to the Commonwealth Ombudsman, AFP officers may make such a disclosure externally if an internal investigation was inadequate or not completed in the relevant time limit, or if the response to an internal investigation was inadequate. However, an external disclosure may not be made if it would reveal 'sensitive law enforcement information' (under subsection 41(2), 'information the disclosure of which is reasonably likely to prejudice Australia's law enforcement interests' including those listed in the subsection).

Potential amendments

As was the case with the offences relating to SIOs, some stakeholders, particularly media organisations, have objected to the proposed offence relating to DNSWs. A joint submission from a range of media organisations and a separate submission from the Media, Entertainment and Arts Alliance both suggest that proposed section 3ZZHA of the *Crimes Act* be dropped altogether or, as an alternative, amended to include an exception for public interest disclosures.

In its 17 October 2014 report, the Parliamentary Joint Committee on Intelligence and Security recommended the inclusion of some additional exceptions to the proposed offence relating to DNSWs. However, the recommended additions did not include an exception for public interest disclosures other than to the Commonwealth Ombudsman.

If the Parliament determines that in order to address public interest disclosures, an amendment to the offence relating to DNSWs is appropriate, it would be logical for equivalent amendments to be made to the offences relating to SIOs in the *ASIO Act* and those relating to controlled operations in the *Crimes Act* to provide a consistent approach to these types of disclosures.

Further reading

For further information on the application of the *Criminal Code* to Commonwealth offences, see:

- I Leader-Elliott, *The Commonwealth Criminal Code: a guide for practitioners*, Attorney-General's Department (AGD) and Australian Institute of Judicial Administration, Canberra, 31 March 2002 and
- AGD, *A guide to framing Commonwealth offences, infringement notices and enforcement powers*, Australian Government, Canberra, updated September 2011.

© Commonwealth of Australia

Creative Commons

With the exception of the Commonwealth Coat of Arms, and to the extent that copyright subsists in a third party, this publication, its logo and front page design are licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Australia licence.

Disclaimer: The views expressed in this Quick Guide do not reflect an official position of the Australian Parliamentary Library, nor do they constitute professional legal opinion.