Professor Clive Walker
School of Law, University of Leeds

Inquiry into section 35P of the Australian Security Intelligence Organisation Act 1979

Submission to the Independent Security Law Monitor

3 April 2015

1 Section 35P of the Australian Security Intelligence Organisation Act 1979 ('ASIO Act') establishes offences for the disclosure of information relating to a 'special intelligence operation' undertaken by ASIO, where authorised by the Commonwealth Attorney-General under Division 4 of Part III of the ASIO Act. The special intelligence operations scheme, including section 35P, commenced on 30 October 2014. By section 35P:

'Unauthorised disclosure of information
(1) A person commits an offence if:
(a) the person discloses information; and
(b) the information relates to a special intelligence operation.
Penalty: Imprisonment for 5 years.
Note: Recklessness is the fault element for the circumstance described in paragraph (1)(b)--see section 5.6 of the Criminal Code .

Unauthorised disclosure of information--endangering safety, etc.
(2) A person commits an offence if:
(a) the person discloses information; and
(b) the information relates to a special intelligence operation; and
(c) either:
(i) the person intends to endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation; or
(ii) the disclosure of the information will endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation.
Penalty: Imprisonment for 10 years.
Note: Recklessness is the fault element for the circumstance described in paragraph (2)(b)--see section 5.6 of the Criminal Code .

Exceptions
(3) Subsections (1) and (2) do not apply if the disclosure was:
(a) in connection with the administration or execution of this Division; or
(b) for the purposes of any legal proceedings arising out of or otherwise related to this Division or of any report of any such proceedings; or
(c) in accordance with any requirement imposed by law; or
(d) in connection with the performance of functions or duties, or the exercise of powers, of the Organisation; or
(e) for the purpose of obtaining legal advice in relation to the special intelligence operation; or
(f) to an IGIS official for the purpose of the Inspector-General of Intelligence and Security exercising powers, or performing functions or duties, under the Inspector-General of Intelligence and Security Act 1986 ; or
(g) by an IGIS official in connection with the IGIS official exercising powers, or performing functions or duties, under that Act.
Note: A defendant bears an evidential burden in relation to the matters in this subsection--see subsection 13.3(3) of the Criminal Code.

Extended geographical jurisdiction
(4) Section 15.4 of the Criminal Code (extended geographical jurisdiction--category D) applies to an offence against subsection (1) or (2).
(5) Subsection (4) does not, by implication, affect the interpretation of any other provision of this Act.'

2 The purpose of this submission is to assist the Inquiry by providing a comparative perspective based on UK law. UK counter-terrorism law has been a prime influence in the shaping of Australian law since 9/11. However, section 35P cannot be directly linked to a precedent in UK law since there is no equivalent provision for a 'special intelligence operation' as undertaken by security agencies. The explanation is that the security agencies in the UK are kept in the background compared to the police. They have been conferred with relatively few (though potentially broad) executive powers which allow intrusion upon property,[1] but their impact upon privacy is of course the subject of as much controversy in the UK as elsewhere in the light of the Edward Snowden revelations.[2] Perhaps the starkest contrast with Australia is that the security agencies have never been granted powers to detain and question equivalent to those inserted by the Australian Security Intelligence Organisation Legislation (Terrorism) Amendment Act 2003 (Cth) in relation to Questioning Warrants (ASIO Act, Pt III Div 3 sub-div B) and Questioning and Detention Warrants (ASIO Act, Pt III Div 3 sub-div C). Such powers would not sit well with the UK's conventional division of responsibilities between police and security agencies which reflects appropriate capabilities and training and also the mechanisms for accountability. The same reticence would apply in the UK to any proposal for a new legislative code for 'special intelligence operations'.

3 As far as the specific mischief of the unauthorised disclosures of information about terrorism operations are concerned, the nearest equivalent UK offence is section 39 (as amended) of the Terrorism Act 2000 ('TA 2000'):

'39 Disclosure of information, &c
(1) Subsection (2) applies where a person knows or has reasonable cause to suspect that a constable is conducting or proposes to conduct a terrorist investigation.

(2) The person commits an offence if he
(a) discloses to another anything which is likely to prejudice the investigation, or
(b) interferes with material which is likely to be relevant to the investigation.

(3) Subsection (4) applies where a person knows or has reasonable cause to suspect that a disclosure has been or will be made under any of sections 19 [to 21B] [or 38B.]

(4) The person commits an offence if he
(a) discloses to another anything which is likely to prejudice an investigation resulting from the disclosure under that section, or

[1] See Intelligence Services Act 1994, s 5(1): 'No entry on or interference with property or with wireless telegraphy shall be unlawful if it is authorised by a warrant issued by the Secretary of State under this section.' Compare the Police Act 1997, Pt.III.
[2] Interception of communications powers are mainly contained in the Regulation of Investigatory Powers Act 2000.

(b) interferes with material which is likely to be relevant to an investigation resulting from the disclosure under that section.

(5) It is a defence for a person charged with an offence under subsection (2) or (4) to prove

(a) that he did not know and had no reasonable cause to suspect that the disclosure or interference was likely to affect a terrorist investigation, or

(b) that he had a reasonable excuse for the disclosure or interference.

(6) Subsections (2) and (4) do not apply to a disclosure which is made by a professional legal adviser

(a) to his client or to his client's representative in connection with the provision of legal advice by the adviser to the client and not with a view to furthering a criminal purpose, or

(b) to any person for the purpose of actual or contemplated legal proceedings and not with a view to furthering a criminal purpose.

[(6A) Subsections (2) and (4) do not apply if

(a) the disclosure is of a matter within section 21D(2) or (3)(a) (terrorist property: tipping off), and

(b) the information on which the disclosure is based came to the person in the course of a business in the regulated sector.]

(7) A person guilty of an offence under this section shall be liable

(a) on conviction on indictment, to imprisonment for a term not exceeding five years, to a fine or to both, or

(b) on summary conviction, to imprisonment for a term not exceeding six months, to a fine not exceeding the statutory maximum or to both.

(8) For the purposes of this section

(a) a reference to conducting a terrorist investigation includes a reference to taking part in the conduct of, or assisting, a terrorist investigation, and

(b) a person interferes with material if he falsifies it, conceals it, destroys it or disposes of it, or if he causes or permits another to do any of those things.

[(9) The reference in subsection (6A) to a business in the regulated sector is to be construed in accordance with Schedule 3A.]

4 The following book extract from para.4.90 of Clive Walker, *The Anti-Terrorism Legislation* (Third edition, Oxford University Press, Oxford, 2014) considers the application of section 39 and related measures:

'Section 39 of the TA 2000 provides for two sets of offences to discourage or penalize disclosures that may damage the effectiveness of ongoing terrorist investigations. The offences may affect both those conducting the investigations, including civilian aids of the security authorities, and also outsiders such as journalists. Disclosures within the regulated

sector are exempted from s 39 since they fall under the corresponding strict liability offence of tipping off under s 21D.[3] These offences under s 39 add to those under the Official Secrets Act 1989, s 4 of which was raised against the disclosure of a Joint Terrorism Analysis Centre document in *R v Thomas Lund-Lack.*[4] A charge of misconduct in public office was sustained against DCI April Casburn, based in the National Terrorist Financial Investigation Unit, for disclosure of non-terrorist information.[5] ... No charges have been reported under s 39.'

5 The details of section 39 reveal that there has been a specific legislative response to unauthorised disclosures which might hamper anti-terrorism operations, but it is set in terms which are both broader and narrower than section 35P of ASIO. Section 39 is broader in that it is not confined to a 'special intelligence operation' but can relate to any terrorist investigation. By section 32:

'In this Act 'terrorist investigation' means an investigation of
(a) the commission, preparation or instigation of acts of terrorism,
(b) an act which appears to have been done for the purposes of terrorism,
(c) the resources of a proscribed organisation,
(d) the possibility of making an order under section 3(3), or
(e) the commission, preparation or instigation of an offence under this Act or under Part 1 of the Terrorism Act 2006 other than an offence under section 1 or 2 of that Act.'

This breadth of scope is reinforced by the applicability of the even more expansive Official Secrets Act 1989, section 4(1), by which 'A person who is or has been a Crown servant or government contractor is guilty of an offence if without lawful authority he discloses any information, document or other article to which this section applies and which is or has been in his possession by virtue of his position as such.'

6 At the same time, the UK legislation is significantly narrower than section 35P in two respects. One is that there is generally a requirement of damage which must result from the disclosure; mere disclosure is not enough. This element is reflected in the words, 'prejudice' or 'interferes' in section 39(2). Likewise, under the Official Secrets Act 1989, section 4(2):

'This section applies to any information, document or other article
(a) the disclosure of which
(i) results in the commission of an offence; or
(ii) facilitates an escape from legal custody or the doing of any other act prejudicial to the safekeeping of persons in legal custody; or
(iii) impedes the prevention or detection of offences or the apprehension or prosecution of suspected offenders; or

[3] s 39(6A). See Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007, SI 2007/3398. The regulated sector is as defined by Sch 3A: s 39(9).
[4] *The Times* 28 July 2007 p 32.
[5] < http://www.judiciary.gov.uk/judgments/april-casburn-sentencing-remarks-01022013/ >, Southwark Crown Court, 1 February 2013.

(b) which is such that its unauthorised disclosure would be likely to have any of those effects.'

Disclosure *per se* seems to suffice for section 35P, though intent to cause damage results in a more serious offence.

7 The second aspect of narrowing is the recognition that wide public interests may be raised by way of justification for disclosure under section 39, including the public interest in investigative journalism. This point is obliquely recognised in section 39(5)(b) by which there may be 'a reasonable excuse for the disclosure or interference'. The value of expressive rights is also safeguarded by the overlap of article 10 in Schedule 1 of the Human Rights Act 1998, which must be taken into account both in relation to section 39 and the Official Secrets Act 1989. The point was explored under the Official Secrets Act 1989 in *R v Shayler*.[6] The defendant, a former member of the security service, was charged with unlawful disclosure of documents and information contrary to sections 1 and 4 of the Official Secrets Act 1989. He asserted that his disclosures had been made in the public and national interest. The judgment of the House of Lords sustains that offences under the Official Secrets Act 1989 are sufficiently clear to qualify as being 'prescribed by law' under Article 10(2) of the European Convention as valid restrictions on freedom of expression. In addition, the restriction on freedom of expression could be consistent with article 10(2) when it was directed to one or more of the objectives there specified and was shown to be necessary in a democratic society. In *Shayler*, the restriction was directed towards relevant objectives specified in article 10(2), namely, the need to preserve the secrecy of information relating to intelligence and military operations in order to counter terrorism, criminal activity, hostile activity and subversion. Nevertheless, the ban on disclosure even by a former member of the service did not amount to an absolute ban, and disclosures *per se* are not all to be stifled. Though Shayler was properly convicted, it should be emphasised that Shayler was not a journalist and that the journalists to whom he disclosed his materials were not prosecuted.

8 In conclusion, this comparative exercise points towards two conclusions. One is that the use of the criminal law to protect sensitive information relating to counter-terrorism is justifiable. However, the second point is that the criminal law should not be applied to excess. It is important to allow for the raising of reasonable excuses by way of a defence, including the public interest in the disclosure of wrongdoing. This recognition is insufficiently reflected in section 35P. As a result, it may be argued that section 35P is unprincipled, especially since Australian Commonwealth law lacks any general domestic law statement of protection equivalent to article 10 of the Human Rights Act 1998, despite endorsing the value of free speech at common law and in international law. A more pragmatic reason for the recognition of the value of the public interest is that, in the absence of any statutory statement, these issues will be raised in an unstructured and messier way, perhaps resulting in what the state authorities might view as perverse jury acquittals.[7]

[6] [2002] UKHL 11.
[7] See *R v Ponting* (1985) *The Times* 29 January.