# SPECIAL INTELLIGENCE OPERATIONS AND FREEDOM OF THE PRESS

KEIRAN HARDY and GEORGE WILLIAMS

The federal coalition government under Prime Ministers Tony Abbott and Malcolm Turnbull has been active in having Parliament enact a range of new anti-terrorism laws. These laws have been introduced in response to the problem of 'foreign fighters' returning from the conflicts in Iraq and Syria, as well as the threat of homegrown terrorism by individuals who are inspired by the actions of Islamic State.

Measures enacted by the federal Parliament to combat these threats include a new power to revoke the citizenship of dual nationals who are involved with terrorism and an offence of entering any area declared by the federal government to be a no-go zone.[1] Laws making amendments in a wide range of other areas have also been framed as a response to this increased threat of terrorism, including stronger offences for intelligence whistleblowing and a mandatory metadata retention regime.

A number of these measures have been controversial, including due to their impact upon freedom of speech and freedom of the press. A new offence of advocating terrorism, for example, provides for up to five years jail for any person who promotes or encourages the doing of a terrorist act or terrorism offence.[2] Imprisonment can result merely from a person's speech, and the person need not intend any other person to commit a terrorism act or terrorism offence.[3]

One of the most hotly debated of these laws is a new 'special intelligence operations' regime. That regime grants immunity from civil and criminal liability to Australian Security Intelligence Organisation ('ASIO') officers during the course of specially approved undercover operations. Attached to this regime are disclosure offences, found in section 35P of the *Australian Security Intelligence Organisation Act 1979* (Cth) ('ASIO Act'), which impose penalties of up to 10 years for disclosing any information that relates to a special intelligence operation.

Section 35P attracted such a strong reaction, especially from parts of the press on the grounds that it would prevent media reporting on ASIO's activities, that the government immediately referred the legislation for review by the newly appointed Independent National Security Legislation Monitor ('Independent Monitor'), Roger Gyles. Gyles' report was released in early 2016,[4] and the government has since indicated that it will introduce a range of amendments to the legislation based on his concerns and recommendations.

In this article we consider the potential impact of s 35P on journalists and whether the changes recommended by the Independent Monitor are sufficient to remedy deficiencies in the provision. One of Gyles' key recommendations was to separate the offence so that it applies to two different categories of people: 'insiders' (intelligence officers and contractors) and 'outsiders' (journalists and any other person).[5] The Independent Monitor did not recommend any changes to s 35P as it relates to insiders, so we focus below on how the amended version of the offence will apply to media reporting. We conclude that the proposed amendments will do little to reduce the impact of s 35P on press freedom, and that more significant changes are required.

## Special intelligence operations and s 35P

The *National Security Legislation Amendment Act (No 1) 2014* (Cth) was the first of three tranches of national security legislation introduced by the Abbott government in 2014. Since then, a fourth tranche has been enacted which allows the Minister for Immigration to strip the citizenship of dual citizens involved with terrorism, and a fifth tranche will soon be passed which will allow control orders to be imposed on children as young as 14.

The *National Security Legislation Amendment Act* introduced a special intelligence operations regime. This regime gives the Attorney-General a power to grant ASIO officers immunity from civil and criminal liability in regard to specified activities. Such authorisations may be granted if the Attorney-General is satisfied on reasonable grounds that an operation 'will assist the Organisation in the performance of one or more special intelligence functions'.[6] Special intelligence functions are defined according to ASIO's normal intelligence gathering responsibilities, so this will not in practice pose a barrier to authorisation being granted. The Attorney-General must also be satisfied that any unlawful activity will be limited to the maximum extent necessary, and that any ASIO officers involved will not induce a person to commit a criminal offence.[7] Immunity cannot be granted in relation to conduct which would cause death or serious injury, constitute torture, cause serious property damage or involve the commission of a sexual offence.[8]

REFERENCES

1. *Australian Citizenship Amendment (Allegiance to Australia) Act 2015* (Cth); *Criminal Code Act 1995* (Cth), s 119.2

2. *Criminal Code Act 1995* (Cth), s 80.2C(3).

3. *Criminal Code Act 1995* (Cth), s 80.2C(1)(b).

4. Independent National Security Legislation Monitor, *Report on the Impact on Journalists of s 35P of the ASIO Act* (2015).

5. Ibid 3.

6. *Australian Security Intelligence Organisation Act 1979* (Cth), s 35C(2)(a).

7. *Australian Security Intelligence Organisation Act 1979* (Cth), s 35C(2).

8. *Australian Security Intelligence Organisation Act 1979* (Cth), s 35C(2)(e).

*A key problem for journalists is that it is difficult for them to know whether in their reporting they are complying with this law.*

Section 35P criminalises the disclosure of information relating to special intelligence operations. It provides:

(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.

Under an aggravated version of the offence in subsection (2), the penalty is increased to 10 years if the disclosure would endanger the health or safety of any person or prejudice a special intelligence operation, or if the person intends such results.

Section 35P is expressed in broad and general terms. As Attorney General George Brandis has said, section 35P 'applies generally to all citizens'.[9] It does not discriminate between people who seek to harm Australia's security by revealing secret information, and journalists and whistleblowers who shine a spotlight on government wrongdoing, incompetence or even the death of an Australian citizen at the hands of an intelligence officer. No exceptions are made for such communications. The effect is to criminalise media reporting and other disclosures about special intelligence operations which may be in the public interest.

A key problem for journalists is that it is difficult for them to know whether in their reporting they are complying with this law. Special intelligence operations are by their nature covert, and the information that cannot be disclosed under s 35P covers these operations and anything that 'relates to' them. This means that the ban extends to other, connected operations by ASIO and agencies such as the Australian Federal Police.

All this can create doubt in the mind of a journalist about whether they can publish a story, both in relation to special intelligence operations and national security issues more generally. If, for example, reporters learn of dawn raids on the houses of terrorist suspects, they may decline to publish that information on the basis that it could relate to a special intelligence operation. As a result, the offence is likely to have a significant chilling effect on the freedom of media outlets to report on counter-terrorism operations and other national security matters. This was noted in a submission to the Independent Monitor by a coalition of media organisations including the ABC, SBS, Fairfax Media and NewsCorp. Those organisations argued that uncertainty surrounding s 35P 'will expose journalists to an unacceptable level of risk and consequentially have a chilling effect on the reportage of all intelligence and national security material'.[10]

This chilling effect is likely to be be further aggravated by the third tranche of national security legislation introduced by the Abbott government in 2014,[11] which created a mandatory metadata retention regime. Under that regime, details of a journalist's phone calls and emails may be accessed by ASIO or the police to investigate a possible breach of s 35P. As metadata reveals the time, place, and recipient of a phone call, SMS or email, such information could be used to identify a journalist's confidential source, inside an intelligence agency or otherwise. Additional protections for journalists were added to the legislation through a regime for issuing journalist information warrants,[12] but journalists will not be able to contest applications for these warrants, as the collection of metadata is a process which is kept secret from the person being investigated. Indeed, a journalist who discovered that a warrant was being issued would face two years in prison for revealing that fact.[13]

In response to such concerns, Attorney-General George Brandis reassured the public that a journalist would never 'be prosecuted for doing their job'.[14] He also issued a directive to the Commonwealth Director of Public Prosecutions that no prosecution under s 35P will proceed against a journalist unless federal prosecutors have consulted with and obtained the consent of the Attorney-General of the day. These are welcome assurances, although they still leave the possibility of prosecuting journalists open to executive discretion. Ongoing concerns surrounding the possible application of s 35P to journalists also demonstrate that these assurances are not likely to prevent the legislation from having a chilling effect on free press.

Brandis highlighted a problem, rather than solved it. Journalists must be free to report on matters of public interest without seeking the permission of the government. They should not have to operate under the shadow of a jail term that can only be lifted at the discretion of a minister. In any event, Brandis' concession is a frail shield. Although he has made this commitment, it is not clear that future Attorneys-General (from either side of politics) will stand by the same promise. In particular, it is not clear that Brandis or future Attorneys-General would honour this commitment if a journalist disclosed information that was deeply embarrassing to the government. After all, what a government may wish to see suppressed can

9. George Brandis and Malcolm Turnbull, 'Press Conference Announcing the Introduction of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014' (Joint Press Conference, 30 October 2014).

10. Joint Media Organisations, Submission No 27 to Independent National Security Legislation Monitor, *Inquiry into Section 35P of the ASIO Act*, 22 April 2015, 5

11. *Telecommunications (Interception and Access) Data Retention (Amendment) Act 2015* (Cth).

12. *Telecommunications (Interception and Access) Act 1979* (Cth), ss 180Q, 180T.

13. *Telecommunications (Interception and Access) Act 1979* (Cth), s 182A.

14. Brandis and Turnbull, above n 9.

be exactly the sort of information that the community needs to hear.

Brandis' response also assumes that the government and the media have the same concept of what journalists ought to be reporting. While saying that the section is not directed at journalists, he indicated that s 35P is directed at a 'Snowden' type situation,[15] in which an intelligence employee or contractor contacts journalists to release sensitive national security information to the public. The provision is therefore directed at journalists, to the extent that journalists might be involved in Snowden-type scenarios. It is doubtful that in such circumstances the government would refuse to prosecute the individuals who played a key role in disclosing sensitive information. This is not to say that a journalist who discloses information in such circumstances with the intention of harming Australia's national security should be immune from criminal penalty. Rather, the point is that some Snowden-style disclosures may reveal issues of significant public concern, but be precisely the kind of information that the government wants to suppress. An example of this was the revelations from the Snowden materials about Australian intelligence agencies spying on senior members of the Indonesian government.

## Report of the Independent Monitor

The *National Security Legislation Amendment Act* was enacted by Parliament after receiving bipartisan support. Despite such bipartisanship, the enactment of s 35P provoked a fierce reaction from segments of the press. For example, the offence was criticised by the Media Entertainment and Arts Alliance as 'an outrageous attack on press freedom' and 'not worthy of a healthy, functioning democracy'.[16]

The leader of the opposition, Bill Shorten, responded to such concerns by writing to Prime Minister Abbott requesting that the section be referred to the Independent Monitor for review. Abbott acceded to the request. This produced an inversion of the normal lawmaking process, whereby questions as to the proper scope of legislation are resolved prior to enactment. Instead, remarkably, a criminal sanction imposing penalties of up to 10 years' imprisonment was enacted in a form so troubling that it required immediate review. This set up a similar scenario to that of 2005, when controversial sedition laws were enacted on the understanding that those laws would immediately be referred to the Australian Law Reform Commission for review. Significantly, in contrast to the speedy passage of the *National Security Legislation Amendment Act* through Parliament (with only three days of debate in the Senate and one in the House of Representatives) the process of review of s 35P consumed more than a year (from the referral to the Independent Monitor in December 2014 to the publishing of his report in February 2016, and even this does not include the time still being taken to enact amendments based upon the report).

The report of the Independent Monitor addressed the justifications for the special intelligence operation regime as a whole. The government initially justified the regime on the grounds that Australian Federal Police have the power to undertake 'controlled operations', and that similar powers should be extended to ASIO officers in response to the threat of foreign fighters. The controlled operations regime in Part IAB of the *Crimes Act 1914* (Cth) provides Australian Federal Police officers with immunity for engaging in conduct which is necessary for undercover 'sting' operations but technically unlawful — such as possessing child pornography or illicit drugs. Disclosure offences akin to those in s 35P apply to the controlled operations regime.[17]

The Independent Monitor concluded that the existence of the controlled operations regime is not sufficient to justify ASIO having similar powers, as federal police deal with a much wider range of crimes and are involved in gathering evidence for criminal prosecution rather than intelligence gathering. He also concluded that there was 'no clear or convincing external precedent' from other countries that would justify ASIO having such powers.[18] Indeed, no such regime operates in the United Kingdom, United States or New Zealand.[19]

Given this, it is peculiar that Gyles supported the continuing operation of the special intelligence operations regime. He did so on the basis that ASIO officers could be tempted 'to do "whatever it takes" to secure the nation, which could involve cutting corners or more serious breaches'.[20] He alluded to torture as one of these possibilities, noting controversies over interrogation methods used by different intelligence agencies around the world.[21] He added that the regime, by providing immunity to ASIO officers, 'makes unauthorised activity less likely and not defensible if it occurs'.[22]

This is a weak and unfortunate justification of a regime that is designed to allow ASIO officers to engage in unlawful activity. Indeed, it is reasonable to assume that the regime makes it *more*, not less, likely that ASIO officers will engage in unlawful acts. Such conduct will now be defensible precisely because ASIO officers are protected from criminal liability, and because s 35P prevents any public discussion of such matters. As for the possibility of suspects being tortured, the regime now formally excludes the possibility that ASIO officers could receive immunity for such conduct.[23] However, if a suspect were to be tortured outside the terms of an operation, s 35P would still prevent the public from ever learning of that fact where this information 'relates' to the operation.

While Gyles accepted the need for the special intelligence operations regime, he nonetheless found that changes to s 35P were required. The structural change recommended is to redesign s 35P so that it targets two different categories of people: 'insiders' (intelligence employees and contractors) and 'outsiders' (journalists and any other person).[24]

15. Ibid.

16. Media, Entertainment and Arts Alliance, MEAA Says National Security Law an Outrageous Attack on Press Freedom in Australia (26 September 2014) <http://www.abc.net.au/mediawatch/transcripts/1436_meaa.pdf>; Christopher Warren and Mike Dobbie, Surveillance State Seizes Its Chance, The Walkley Foundation (10 April 2015) <http://walkleys.com/surveillance-state-seizes-its-chance/>.

17. *Crimes Act 1914* (Cth), ss 15HK, 15HL.

18. Independent National Security Legislation Monitor, above n 4, 19.

19. The Canadian Parliament has recently enacted broad powers which provide officers of the Canadian Security Intelligence Service with the power to take measures to 'reduce' threats to the security of Canada: *Anti-Terrorism Act*, RSC 1985, c C-51, s 42. These powers are similar to the Australian regime insofar as Canadian officers are able to take any measures other than those which cause death or bodily harm, pervert the course of justice, or violate the sexual integrity of an individual.

20. Independent National Security Legislation Monitor, above n 4, 20.

21. Ibid.

22. Ibid 21.

23. *Australian Security Intelligence Organisation Act 1979* (Cth), s 35C(2)(e).

24. Independent National Security Legislation Monitor, above n 4, 3.

*The appropriate way to reduce the impact of s 35P on press freedom is to introduce a public interest exemption into the offence.*

The Independent Monitor recommended that an outsider not be liable to punishment under s 35P unless they are reckless as to whether the disclosure will endanger health or safety or prejudice a special intelligence operation.[25] Recklessness means that the person is aware of a 'substantial risk' of those circumstances arising, and the person chooses to publish the information anyway.[26]

This will make it more difficult to prosecute journalists compared to the offence as currently drafted. However, it does not address the major issue with the offence, which is that s 35P does not provide any scope for journalists to disclose information in the public interest. It may be that a journalist is aware of a substantial risk that disclosing information may prejudice an operation, but believes in good conscience that the public should nonetheless be informed about some unlawful or inhumane conduct in which ASIO officers are involved (such as harming a suspect, stealing money or property from a suspect's home, or using information gained during the operation to blackmail a person for financial advantage).

A second amendment will relate to the aggravated version of the offence for outsiders, and require that the person *knows* the disclosure will endanger health or safety or prejudice a special intelligence operation. This will result in somewhat awkward drafting, to require a person's knowledge of circumstances which do not yet exist and which may take some time to occur. A preferable alternative would be to require that the person *intended* to cause such results. This would be consistent with recommendations by the Australian Law Reform Commission that the criminal law should be triggered for disclosing information only when the person intends in some way to harm an essential public interest, such as security or defence.[27]

Finally, the Independent Monitor recommended that the offences include an exemption for outsiders who re-report information which has already been disclosed by others.[28] This exemption will have little practical effect, as it is unlikely that a journalist would be prosecuted for re-reporting information that is the public domain. The target of any such prosecution is likely instead to be the person who first revealed information, and the journalist who first reports it.

In any case, it is not clear that the re-reporting of information would have been criminalised by the offence as originally drafted. A court may interpret the 'disclosure' of information to mean disclosure in the first instance to another person or the general public, and not the mere repeating of information that was already in the public domain.

Whereas the government has supported the other changes in the terms recommended by the Independent Monitor, it has indicated that the exemption for re-reporting will apply only to those who take reasonable steps to ensure that the secondary publication is not likely to cause harm.[29] This will place a higher burden on journalists defending themselves from prosecution. It will not be enough for a journalist to show that the information was already in the public domain; a journalist would also need to demonstrate that positive steps to avoid a risk of harm were taken prior to re-publication.

## A public interest exemption?

The changes proposed by the Independent Monitor are not sufficient to address the primary concerns about s 35P. Journalists will still face five years in prison for disclosing any information relating to special intelligence operations where they are reckless as to the harm that might be caused by disclosure. While this does reduce the circumstances under which journalists might be prosecuted under s 35P, it is unlikely to reduce the significant chilling effect that the offence is likely to have on media outlets. It would still take a brave journalist to report any information relating to such an operation, as they would be risking five years in prison for 'recklessly' causing harm.

The appropriate way to reduce the impact of s 35P on press freedom is to introduce a public interest exemption into the offence. Such an exemption need not be drafted broadly to allow the disclosure of *any* information which a court considers to be in the public interest. It could be drafted narrowly to permit the disclosure of information relating to special intelligence operations by professional media organisations where such disclosure would reveal serious misconduct by ASIO officers — such as torture, blackmail, large-scale corruption or activities which caused a significant danger to members of the public. The availability of disclosure on specific grounds such as these could be set out in the legislation.

The Independent Monitor recognised that a public interest exemption would have been a useful addition to the offence as currently drafted. However, he considered such an amendment to no longer be necessary given the higher fault requirements to

25. Ibid.

26. *Criminal Code Act 1995* (Cth), s 5.4.

27. ALRC, *Secrecy Laws and Open Government in Australia*, Report No 112 (2009) 160.

28. Independent National Security Legislation Monitor, above n 4, 3-4.

29. George Brandis, 'Government Response to INSLM Report on the Impact on Journalists of s 35P of the ASIO Act' (Media Release, 2 February 2016).

be introduced to the offence.[30] This reasoning is unconvincing, as the higher fault requirements will require only that the person recklessly or knowingly caused harm. These will set a higher bar for prosecution, but they will not provide any greater scope for journalists to disclose information in the public interest. A prosecution under s 35P could still succeed, for example, where a journalist revealed that ASIO officers had tortured a suspect during a special intelligence operation, as the journalist may have recklessly or knowingly prejudiced that operation.

As such, s 35P will continue to prevent the disclosure of information of which there is a significant need for the public to be informed. This is not to say that any disclosure that would keep the public usefully informed about ASIO's activities should be permitted. Rather, the goal would be to draft a public interest exemption which provides an adequate 'release valve' in the legislation for circumstances where ASIO officers cross the line into serious criminal activity or inhumane conduct. Such circumstances would hopefully be rare, but reporting on such matters should not be presumptively excluded.

## Conclusion

Australian citizens have a right to know if their intelligence services engage in wrongful, corrupt or unlawful conduct in the name of protecting the nation's security. Unfortunately, s 35P currently prevents this in regard to special intelligence operations, subjecting journalists to up to 10 years imprisonment for disclosures that may be in the public interest. The problems raised are obvious, especially in regard to their inconsistency with freedom of the press.

Unfortunately, the Independent Monitor failed to suggest reforms that remedy the problem. The proposals to restructure the offence and introduce additional fault elements offer an improvement, but do not go far enough. In particular, they still leave open the possibility of journalists being jailed for reporting matters that are clearly in the public interest. What is instead required is an amendment of the section to introduce a public interest exemption that protects journalists from prosecution in specified circumstances. A change along these lines would strike an appropriate balance between protecting the secrecy of the special intelligence operation regime and allowing journalists to report responsibly on issues of significant public importance.

**KEIRAN HARDY** is a lecturer in the School of Criminology and Criminal Justice and a member of the Griffith Criminology Institute, Griffith University. **GEORGE WILLIAMS** is the Dean, Anthony Mason Professor, and a Scientia Professor at the Faculty of Law, University of New South Wales.



email: <k.hardy@griffith.edu.au>
<george.williams@unsw.edu.au>

30. Independent National Security Legislation Monitor, above n 4, 27.