GILBERT + TOBIN
CENTRE OF PUBLIC LAW

THE UNIVERSITY OF NEW SOUTH WALES

FACULTY OF LAW

GILBERT + TOBIN CENTRE OF PUBLIC LAW

2 April 2015

The Hon Roger Gyles AO QC
Independent National Security Legislation Monitor
One National Circuit
Barton ACT 2600

Dear Mr Gyles,

Inquiry into section 35P of the ASIO Act

Thank you for the opportunity to make a submission to this inquiry. We do so in our capacity as members of the Gilbert + Tobin Centre of Public Law at the Faculty of Law, University of New South Wales. We are solely responsible for the views and content in this submission.

Section 35P of the *Australian Security Intelligence Organisation Act (1979)* (Cth) (ASIO Act), in criminalising the disclosure of any information relating to Special Intelligence Operations (SIOs), poses a clear risk to freedom of the press. The offence prohibits journalists from reporting on SIOs, even where this would reveal that ASIO officers were involved in substantial wrongdoing or unlawful conduct during the course of an operation.

SYDNEY 2052 AUSTRALIA
Telephone: +61 (2) 9385 9654
Facsimile: +61 (2) 9385 1175
www.gtcentre.unsw.edu.au

While several other offences apply to the disclosure of national security information,[1] s 35P is deserving of special attention in that it attaches to a unique undercover operations regime. No comparable nation has seen it necessary to grant the same level of immunity to officers of their domestic security service for committing unlawful acts during undercover operations.[2] The SIO regime is based on the controlled operations regime for Australian Federal Police (AFP) officers,[3] but ASIO is not a law enforcement organisation and the SIO regime does not in any case recreate the same accountability mechanisms as those applying to controlled operations.[4]

Below we set out our major concerns with s 35P, including how it relates to metadata and whistleblower legislation. We then suggest solutions to reduce the impact of s 35P on press freedom.

1. Impact on Journalists

Section 35P of the ASIO makes it an offence punishable by five years' imprisonment to disclose any information that relates to an SIO.[5] An SIO is a special undercover operation which is approved by the Attorney-General and grants immunity to the ASIO officers involved for conduct engaged in during the course of the operation. Immunity will not be granted in relation to conduct that causes death or serious injury, constitutes torture, involves the commission of a sexual offence, or causes serious property damage.[6] There is also an

[1] See, eg, *Intelligence Services Act 2001* (Cth), ss39-40B; *Australian Security Intelligence Organisation Act 1979* (Cth), s 18; *Criminal Code Act 1995* (Cth), s 91.1; *Crimes Act 1914* (Cth), ss 70, 79. See also Keiran Hardy and George Williams, 'Terrorist, Traitor or Whistleblower? Offences and Protections in Australia for Disclosing National Security Information' (2014) 37(2) *University of New South Wales Law Journal* 784, 796-808.

[2] See *Security Service Act 1989* (UK0 c 5; *New Zealand Security Intelligence Service Act 1969* (NZ), which contain no similar provisions. Canada has recently introduced a Bill which would allow officers of the Canadian Security Intelligence Service (CSIS) to undertake some unlawful activities, but authorisations to do so would only be available on application to a judge of the federal court, and only in relation to a limited range of conduct (including entering private premises, searching for documents or things, and installing listening devices): see Anti-Terrorism Bill, RSC 2015, C-51, cl 21.1.

[3] *Crimes Act 1914* (Cth) pt 1AB.

[4] For example, a controlled operation can only be authorised for an initial period of three months and requires intermittent renewal by the Administrative Appeals Tribunal, whereas an SIO can be authorised at the outset for 12 months: *Crimes Act 1914* (Cth), s 15GH(4)(c)(i), 15GT; *Australian Security Intelligence Organisation Act 1979* (Cth), s 35Dd(1)(d). An overview of the AFP's controlled operations is also provided in an annual report, whereas the same detailed reporting requirements do not apply to SIOs: *Crimes Act 1914* (Cth), s 15HM-N; *Australian Security Intelligence Organisation Act 1979* (Cth), s 35Q. See Australian Federal Police, *Controlled Operations Annual Report 2013-14: Part IAB of the Crimes* (2014).

[5] *Australian Security Intelligence Organisation Act 1979* (Cth), s 35P(1).

[6] *Australian Security Intelligence Organisation Act 1979* (Cth), s 35K(1)(e).

aggravated offence, punishable by 10 years' imprisonment, where a disclosure endangers the health or safety of any person or prejudices an SIO, or where the person intends such results.[7]

For a person to commit an offence under s 35P, they do not need to know that the information relates to an SIO. It is enough that the person is reckless as to that connection (i.e. the person is aware of a 'substantial risk' that the information relates to an SIO, and chooses to disclose it anyway).[8] The information need only relate to an SIO in some minor or indirect way, and the person need not intend to harm national security or the public interest. Section 35P would also apply if a person revealed that ASIO officers had engaged in conduct for which they cannot receive immunity (such as causing serious property damage, or otherwise acting outside the terms of the operation). There are exemptions for information disclosed to the Inspector-General of Intelligence and Security (IGIS) or to a lawyer,[9] but there is no general defence for information disclosed in the public interest.

The broad scope of this offence clearly impacts on the freedom of journalists to report on ASIO's activities. Journalists face five years in prison if they publish any information that relates to an SIO, even where that information is clearly of national interest. For example, a journalist would face criminal penalty for revealing that ASIO officers had physically harmed a suspect during an SIO, or that an SIO posed a risk to the safety of the general public.

Even if the government chooses not to prosecute journalists for such disclosures,[10] s 35P is likely to have a significant chilling effect on press freedom. For example, if reporters are informed about dawn raids on the houses of terrorist suspects, they might decline to publish that information out of fear that it relates to an SIO. Given that a person need only be aware of a 'substantial risk' that the information relates to an SIO,[11] journalists will likely think twice before publishing anything relating to counter-terrorism operations in which ASIO is involved.

---

[7] *Australian Security Intelligence Organisation Act 1979* (Cth), s 35P(2).
[8] *Criminal Code Act 1995* (Cth), s 5.4.
[9] *Australian Security Intelligence Organisation Act 1979* (Cth), s 35P(3)(e)-(g).
[10] In October 2014, the Attorney-General issued a directive to the Commonwealth Director of Public Prosecutions (CDPP) that no prosecution under s 35P will proceed against a journalist unless the CDPP has consulted with and obtained the consent of the Attorney-General of the day: George Brandis, 'Press Conference Announcing the Introduction of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014', 30 October 2014.
[11] *Australian Security Intelligence Organisation Act 1979* (Cth), s 35P(1); *Criminal Code Act 1995* (Cth), s 5.4.

2. Access to Journalists' Metadata

Section 35P will also impact on press freedom as it will trigger the power for ASIO, the AFP and other agencies to access journalists' telecommunications data and identify their confidential sources. Under the new metadata legislation passed by the Federal Parliament, telecommunications service providers are required to retain metadata (including the time, date and source of a communication) for two years.[12] Enforcement agencies (which currently include the AFP, State Police forces and other criminal law enforcement agencies) have access to metadata where doing so is reasonably necessary for the enforcement of the criminal law, to locate missing persons, to enforce a pecuniary penalty or to protect the public revenue.[13] ASIO has access to metadata where doing so is 'in connection with the performance by the Organisation of its functions'.[14]

The metadata legislation requires that enforcement agencies obtain a warrant where a purpose of disclosing metadata would be to identify a journalist's source.[15] An issuing authority may issue a 'journalist information warrant' after weighing the public interest involved in revealing the source's identity.[16] This is an improvement on the original Bill as introduced into Parliament, which did not include any protections for journalists' sources.

However, there are two remaining problems with this procedure. The first is that ASIO need only seek a ministerial (rather than judicial) warrant.[17] As s 35P relates to ASIO's undercover operations, it seems likely that these ministerial warrants would commonly be sought in relation to breaches of that provision. If a journalist published a story which revealed information about an SIO, ASIO would have significant interest in identifying which of its officers communicated that information to the journalist.

The second problem is that the warrant procedure will not necessarily limit the circumstances in which journalists' metadata relating to a source will be accessed. The availability of the power to access journalists' metadata will still depend on the scope of the offences which

[12] *Telecommunications (Interception and Access) Act 1979* (Cth), ss 187A, 187C.
[13] *Telecommunications (Interception and Access) Act 1979* (Cth), ss 176A, 178-179.
[14] *Telecommunications (Interception and Access) Act 1979* (Cth), s 175(3).
[15] *Telecommunications (Interception and Access) Act 1979* (Cth), s 180Q.
[16] *Telecommunications (Interception and Access) Act 1979* (Cth), s 180T(2)(b).
[17] *Telecommunications (Interception and Access) Act 1979* (Cth), s 180J.

trigger that power.[18] Section 35P is a serious criminal offence, and while issuing authorities are required to weigh up the public interest in revealing a journalist's source,[19] it is not up to the issuing authorities to decide that s 35P imposes criminal penalties in unjustified circumstances. If a journalist is suspected of breaching s 35P, an issuing authority would be likely to issue a warrant to enforce that offence, just as he or she would in relation to any other crime.

3. Lack of Whistleblower Protections

Another key concern is the difficulties in seeking whistleblower protections for breaches of s 35P. In the absence of a public interest exemption in the offence, whistleblower legislation could play an important role in ensuring that section 35P is not triggered in circumstances where the information disclosed about SIOs is of significant national interest.

The *Public Interest Disclosure Act 2013* (Cth) (PID Act) establishes a formal whistleblowing scheme for public officials. It provides immunity from civil, criminal and administrative liability for public officials who disclose wrongdoing by government departments according to a specified procedure.[20] The information they disclose must fall within the definition of 'disclosable conduct'.[21] That definition specifies a range of categories, including information about conduct which is unlawful, is an abuse of public trust, or unreasonably results in danger to health or safety of any person.[22] The person must first disclose that information internally, and believe on reasonable grounds that an internal investigation was inadequate, before disclosing that information to a person outside the organisation.[23]

However, this scheme only applies to 'public officials' (including government contractors),[24] so it would not provide immunity to journalists who disclose information in breach of s 35P.

[18] As the disclosure of metadata may be authorised where 'reasonably necessary for the enforcement of the criminal law': *Telecommunications (Interception and Access) Act 1979* (Cth), s 178.
[19] *Telecommunications (Interception and Access) Act 1979* (Cth), s 180T(2)(b).
[20] *Public Interest Disclosure Act 2013* (Cth), s 10.
[21] *Public Interest Disclosure Act 2013* (Cth), s 29.
[22] *Public Interest Disclosure Act 2013* (Cth), s 29.
[23] *Public Interest Disclosure Act 2013* (Cth), s 26.
[24] *Public Interest Disclosure Act 2013* (Cth), ss 26(1)(a), 69.

The PID Act could provide immunity to intelligence officers who disclose information about SIOs to the IGIS or a lawyer,[25] but due to broad exemptions for intelligence information it would be virtually impossible for them to receive immunity for disclosing that information to a journalist.[26] The only circumstances in which this might be possible would be where the officer believes on reasonable grounds that information about an SIO 'concerns a substantial and imminent danger' to health or safety or the environment, and the information disclosed does not reveal any intelligence operations, sources or methods.[27]

4. Solutions

The most direct solution to the issues posed by s 35P would be to exempt journalists from the offence. The Parliamentary Joint Committee on Intelligence and Security (PJCIS) considered this option in its inquiry into the *National Security Legislation Amendment Act (No 1)* (2014), but concluded that such an exemption would grant bloggers and other informal commentators too much scope to damage intelligence operations.[28] These concerns are valid, although it would be possible to restrict such an exemption to those producing news reports 'in a professional capacity',[29] or some similar wording that would allow established media outlets to report responsibly on SIOs.

A more fundamental problem is that exempting journalists from the offence sits uneasily with the idea that the criminal law should apply equally to every person in society. At the same time, there is also precedent for including special provisions for journalists in order to protect freedom of the press. State and national shield laws are one example of this,[30] as is the recent inclusion of a warrant process for obtaining journalists' metadata.[31]

A preferable solution would be to include an exemption in s 35P for information disclosed in the public interest. One of us has examined this possibility in a recent article,[32] and suggested

[25] *Public Interest Disclosure Act 2013* (Cth), s 26(1)(Items 1, 4).
[26] *Public Interest Disclosure Act 2013* (Cth), ss 26(1), 33, 41. See Hardy and Williams, above n 1, 812-815.
[27] *Public Interest Disclosure Act 2013* (Cth), ss 26(1)(Item 3(a)).
[28] Parliamentary Joint Committee on Intelligence and Security (PJCIS), Parliament of Australia, *Advisory Report on the National Security Legislation Amendment Bill (No 1) 2014* (September 2014) 62 [3.101].
[29] This wording has been included in an exemption to the offence of entering or remaining in a 'declared area': *Criminal Code Act 1995* (Cth), s 119.2(3)(f).
[30] *Evidence Act 1995* (Cth), s 126H; *Evidence Act 1995* (NSW), s 126K.
[31] *Telecommunications (Interception and Access) Act 1979* (Cth), ss 180Q, 180J.
[32] Keiran Hardy, 'National Security Reforms and Freedom of the Press' (2015) 3(1) *Griffith Journal of Law and Human Dignity* 1.

that such an exemption could be drafted narrowly in allowing information about SIOs to be disclosed only where it reveals some substantial wrongdoing or unlawful conduct. This exemption could draw on the definition of 'disclosable conduct' in the PID Act, which refers to a range of serious conduct including that which is unlawful or unreasonably dangerous.[33]

However, even if such an exemption is included in the offence it would not address the larger problem – which is that s 35P does not require any intention to prejudice security or the public interest. Journalists will face five years' imprisonment if they reveal any information about an SIO, regardless of the effect of disclosing that information. They will face twice that penalty if the disclosure prejudices an SIO, whether they intend this result or not.[34]

There is a strong argument that the criminal law should only be triggered where somebody intends by disclosing information to harm the public interest.[35] We believe that some intention to prejudice security should be stipulated as an element of the offence.

Finally, it is not clear why the penalty for the base offence in s 35P should be five years' imprisonment, when the penalty for s 15HK of the *Crimes Act 1914* (Cth) (the equivalent disclosure offence attaching to the AFP's controlled operations regime) is only two years' imprisonment.[36] If no intention to harm the public interest is to be specified in s 35P, then the penalty for the base offence should be lowered to two years' imprisonment to ensure parity with the controlled operations legislation.

Yours sincerely,

Dr Keiran Hardy
Research Fellow, Gilbert + Tobin Centre of Public Law, University of New South Wales

Professor George Williams AO
Anthony Mason Professor and Foundation Director, Gilbert + Tobin Centre of Public Law, University of New South Wales

[33] *Public Interest Disclosure Act 2013* (Cth), s 29.
[34] *Australian Security Intelligence Organisation Act 1979* (Cth), s 35P(2)(c)(ii).
[35] Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report No 112 (2009) 9, 138, 160, 324.
[36] *Crimes Act 1914* (Cth), s 15HK(1).