A Secretive State: The Collaery Trial and National Security Disclosures

Australian Public Law - AUSPUBLAW – 6 November 2019

BY KEIRAN HARDY

In August 2019, the intelligence officer known as Witness K indicated he would plead guilty to a conspiracy charge under s 39 of the *Intelligence Services Act 2001* (Cth) (ISA). That section prohibits the disclosure of information acquired or prepared by the Australian Secret Intelligence Service (ASIS). His lawyer, Bernard Collaery, is being charged with the same offence but is contesting that charge in the ACT Supreme Court. Both charges follow revelations that ASIS officers bugged Cabinet offices of the Timor-Leste government during trade negotiations over access to oil and gas reserves in the contested Timor Sea.

The Collaery trial is significant for several reasons. I have previously outlined some of the issues presented by the National Security Information Act, which will prevent Collaery from knowing all the details of the evidence against him. Here, I discuss three broader reasons why the trial is significant. First, it confirms the need for stronger whistleblower protections when sensitive information is disclosed in the public interest. Second, it highlights the dangers of a series of new secrecy offences introduced in response to terrorism since 2014. Third, it reflects an entrenched culture of government secrecy and a disturbing willingness to prosecute whistleblowers who shed light on the questionable activities of government.

Lack of whistleblower protections

Australia has national whistleblower protections in the *Public Interest Disclosure Act 2013* (Cth) (PID Act), but these are unavailable to lawyers, journalists, or private citizens who disclose information in the public interest. In practice, they are also effectively unavailable to intelligence officers, even though they are government employees.

The PID Act grants immunity from civil and criminal liability for public officials – meaning government employees, statutory officeholders or service providers contracted to government – who reveal 'disclosable conduct'. Under s 29, this means conduct that:

- Contravenes a law;
- Perverts the course of justice;
- Involves corruption;
- Constitutes maladministration;
- Constitutes an abuse of public trust;
- Involves the fabrication or falsification of scientific evidence;
- Involves the wastage of public money;
- Unreasonably results in danger to health or safety; or
- Results in a risk to the environment

For the protections to apply, several requirements must be met – the information cannot simply be disclosed to journalists in the first instance or published online. The discloser must first bring the information to the attention of the agency itself or an appropriate investigative body, such as the Ombudsman. Only after that internal disclosure has been made, and the discloser believes on reasonable grounds that the response was inadequate, can the information then be disclosed publicly. The disclosure must not, on balance, be contrary to the public interest, and the discloser must reveal no more information than is necessary to reveal the disclosable conduct. This final requirement means the scheme does not apply to large-scale information dumps in the style of WikiLeaks or Edward Snowden. Rather, the PID Act allows government employees to reveal specific instances of misconduct according to a tightly constrained procedure.

Additional exclusions mean that the PID Act protections are effectively unavailable to intelligence officers, even though they are public officials for the purposes of the scheme. The first exclusion is that conduct connected with the proper functions of intelligence agencies cannot constitute disclosable conduct. This would still allow for the possibility that conduct outside the proper functions of intelligence agencies could be disclosed – for example, if ASIS officers went outside the terms of an undercover operation to torture a suspect or steal money or weapons. However, there is an additional exclusion for 'intelligence information', meaning information that is held by an intelligence agency or would reveal intelligence sources or methods. A valid public interest disclosure cannot include intelligence information, or even information that 'relates to' an intelligence agency. These exclusions effectively reduce the available disclosures for intelligence officers to nought.

The only remote possibility for an intelligence officer to disclose information publicly is to make a valid 'emergency disclosure'. This would involve disclosing information that relates to an intelligence agency – without revealing any agency documents, sources or methods – provided there is a 'substantial and imminent danger to health or safety'. This sets a very high bar. Otherwise, intelligence officers can disclose information only to the Inspector-General of Intelligence and Security (IGIS) or to a lawyer with an appropriate security classification. The IGIS is an independent statutory office with jurisdiction to investigate and monitor the activities of Australia's intelligence agencies. If an intelligence officer believes that the IGIS investigation was inadequate, there is no subsequent option to disclose the information publicly, as would be available for other government employees.

Importantly, as the PID Act applies only to public officials, its protections are not available to lawyers, journalists, or others who might publish information leaked to them by an intelligence officer. Like intelligence officers, lawyers and journalists who disclose sensitive information can be prosecuted under a wide range of secrecy offences.

Making stronger whistleblower protections available to intelligence officers would pose difficult questions of how to balance national security, freedom of speech, and the public interest. Intelligence officers who intend to harm national security by leaking information should certainly be prosecuted. However, the current problem is that whistleblower protections are not available even in circumstances where the misconduct being revealed is egregious, the information is passed on to a legitimate source (like a journalist or member of Parliament) and it is in the public interest for the information to be known.

Expanded secrecy offences

This lack of whistleblower protections is also significant in the context of wide-ranging secrecy offences available under Australian law. Such offences have been a feature of the counter-terrorism laws introduced by the federal Parliament since 9/11. For example, disclosing information about the use of Preventative Detention Orders (PDOs) is punishable by five years' imprisonment (*Criminal Code Act 1995* (Cth), s 105.41). Those powers allow the federal police to detain people for up to 48 hours for the purpose of preventing a terrorist act. An equivalent offence is attached to ASIO's questioning and detention warrants, which allow ASIO to detain individuals for up to one week for coercive questioning. Those are strict liability offences, as they do not require the discloser to intentionally prejudice national security or cause any other harm.

When Islamic State became a major threat to global security in 2014, the federal Parliament

embarked on another period of rapid, voluminous lawmaking in response to terrorism. The first tranche of foreign fighters legislation strengthened existing disclosure offences for intelligence officers under the ISA by increasing the maximum penalties from two to 10 years' imprisonment. In addition, it introduced new offences for 'unauthorised dealing with records', which are punishable by three years' imprisonment. Those offences apply not to disclosures but instead to the copying, transcribing, or retaining of documents.

These changes signalled a crackdown on intelligence whistleblowing following the WikiLeaks and Snowden scandals, and only tangentially responded to the threat at hand. Importantly, they signalled that the government was no longer seeking merely to punish national security disclosures, but to pre-empt those disclosures happening in the first place. Under the new unauthorised dealing offences, it became possible to prosecute an intelligence officer who copies a classified document onto a USB and takes it out of the building (for example) before they pass that information on to anyone else.

The first tranche of foreign fighters legislation also introduced s 35P into the *Australian Security Intelligence Organisation Act 1979* (Cth). Section 35P prohibits disclosures about 'special intelligence operations' (SIOs). SIOs are undercover operations, approved by the federal Attorney-General, which grant ASIO officers immunity from most criminal conduct. The disclosure offence generated substantial backlash from Australian media organisations, given that journalists could be prosecuted for unintentionally revealing information about an ASIO operation. It was amended following review by the Independent National Security Legislation Monitor, and now requires the disclosure to endanger health or safety or prejudice an SIO for a penalty of up to five years' imprisonment to apply. In its original version, that penalty was available regardless of whether the disclosure caused any harm, was likely to cause harm, or the discloser intended any harm to be caused.

More recently, the federal Parliament enacted the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth). That legislation updated secrecy offences in two ways: it amended longstanding disclosure offences for public officials, found previously in the *Crimes Act 1914* (Cth), and it significantly expanded the federal espionage laws. The new espionage offences rely on a broad definition of 'dealing' with information, which means not only communicating information but also receiving, obtaining, copying or possessing it (*Criminal Code Act 1995* (Cth), s 90.1). These new offences mirrored the expanded offences for intelligence officers, as both sets of crimes now aim to pre-empt disclosures rather than merely punish them after the fact.

In addition, the espionage offences rely on a new and very broad definition of national security, which encompasses Australia's 'political, military or economic relations with … other countries' (*Criminal Code Act 1995* (Cth), s 90.4). A maximum penalty of 25 years' imprisonment applies where a person deals with national security information, is reckless as to whether the conduct will prejudice national security, and the conduct will result in the information being made available to a foreign principal (*Criminal Code Act 1995* (Cth), s 91.1(2)). A maximum penalty of 20 years' imprisonment is available even where the information does not of itself relate to national security (*Criminal Code Act 1995* (Cth), s 91.2(2)). These offences mean a journalist or other person could receive a substantial prison sentence merely for receiving information about Australia's international relations, in circumstances where the publication of the information could be read by members of a foreign government.

With the exception of the updated secrecy offences for public officials, none of these offences contain exemptions for journalists or others who disclose information in the public interest. Given that whistleblower protections under the PID Act are not available for journalists or intelligence officers, and that Australia otherwise has no national protection for fundamental rights, such exemptions are needed urgently to protect free speech and freedom of the press. They are particularly important given the pre-emptive operation of many new secrecy offences. Those offences raise the possibility that the offices of a media organisation might be raided merely for journalists receiving information leaked from a government employee, before they even decide to publish it.

These wide-ranging secrecy offences also operate under the shadow of expanded surveillance powers introduced in response to terrorism. In 2015, the federal Parliament introduced a mandatory data retention regime. Those laws require communications service

providers to retain customers' metadata – including the time, date and location of every phone call and instant message – for two years. This information, which can reveal significant personal details about a person's life, can be accessed by enforcement agencies without a warrant.

The metadata laws raised concerns that enforcement agencies could access journalists' metadata, which would reveal their confidential sources. As a result, enforcement agencies must now seek a 'journalist information warrant' from a judge to access a journalist's metadata. However, journalists are not notified of the existence of a warrant, and they cannot contest a warrant in court, as is possible in the UK and other countries.

Compounding these problems are new laws that aim to give police and intelligence agencies access to encrypted communications. The scheme allows Australian law enforcement and intelligence agencies to request mandatory technical assistance from technology companies, including by decrypting communications or modifying consumer products. This generated substantial backlash from the technology industry, including the major multinationals like Google and Facebook. The laws were designed to allow agencies to read the secret communications of terrorist groups on WhatsApp and other platforms, but they raise the possibility that the encrypted communications of journalists might also be accessed to investigate a criminal offence. In response to the metadata laws, digital rights groups recommended that journalists use encrypted applications to protect their sources – a key ethical obligation of their profession.

Culture of secrecy

The Collaery trial is a single prosecution, but it reflects a wider trend in which the federal government has sought to clamp down on the public discussion of national security information. It signals a willingness in government to prosecute whistleblowers for revealing sensitive information, even where the discloser's intention is to promote transparency, accountability and benefit the wider public interest. The definition of what constitutes national security information has also expanded to the point where it no longer relates merely to security, defence or political violence, but to all political and economic relations with other countries.

Expanding secrecy offences and surveillance powers have been made possible by the increased threat of terrorism since 2014, but these issues are not limited to counter-terrorism. No government likes to be criticised, but the current government seems particularly unwilling to have any embarrassing information aired. Refusals of freedom of information (FOI) requests remain at record levels, and a 'closed book' approach to immigration policy remains the government's default position. A culture of secrecy in government, evident since the election of Tony Abbott to the Prime Ministership in 2013, now seems firmly entrenched.

Following recent police raids on the offices of the ABC, a Newscorp journalist and an Australian Signals Directorate officer, the Australian media will be watching the Collaery trial closely. How the trial is handled will also be of interest to the Right to Know Coalition, which is advocating for stronger legal protections for journalists and greater government transparency. In their minds will be the question: which whistleblower will be prosecuted next? Will it be a lawyer, journalist, or a government employee? And could they or their colleagues be prosecuted for receiving information leaked from government, even if they did not seek out that information and would make the editorial decision not to publish? These are all possibilities under Australia's ever-expanding national security laws.

Keiran Hardy is a Postdoctoral Research Fellow in the Griffith Criminology Institute and a Lecturer in the School of Criminology and Criminal Justice at Griffith University

Suggested Citation: Keiran Hardy, 'A Secretive State: The Collaery Trial and National Security Disclosures' on AUSPUBLAW (6 November 2019) <https://auspublaw.org/2019/11/a-secretive-state/(opens in a new tab)>