Critical Essay

BENEFITS, CHALLENGES, AND PITFALLS OF PRIVATE INTELLIGENCE

Mick Palmer, AO, APM†

It was my pleasure to give the opening address at the Privatisation of Intelligence Symposium hosted by Charles Sturt University and the Australian Research Council Centre of Excellence in Policing and Security. In this paper I draw from that address, my policing career and my involvement in key strategic and operational reviews and inquiries on behalf of government. My focus is to discuss from a practitioner's perspective, core concepts of intelligence and information sharing in the Australian context. It is underpinned by the fact that the privatisation of intelligence is a reality and has been for some years. With this as the starting point, I go on to challenge policy concepts that do not recognise this reality and assess the benefits, challenges and pitfalls of the privatisation of intelligenceand intelligence sharing in Australia. I conclude with remarks about what this might portent for future policing and policy leaders.

Keywords: Intelligence, private investigation, need-to-know doctrine, need-to-share doctrine, right-to-know doctrine.

THE AUSTRALIAN CONTEXT

In Australian policing and public services, the extent and nature of outsourcing is a contentious yet significant policy issue. Outsourcing and privatisation are a reality premised on the limitation of government resources to meet an ever expanding public demand for services. The outsourcing or privatisation of intelligence, once considered the sole domain of policing and intelligence agencies, is an inevitable part of Australia's policing and policy future. However, it does need to be examined in light of the reluctance of governments

† Corresponding author: MPAassociates@bigpond.com

in Australia to share intelligence beyond a narrow framework. What is essential is that this narrow framework is broadened to include more complete intelligence sharing with private industry bodies including multi-national corporations who have a legitimate "right-to-know."

From the perspective of being an *inclusionist* and not an *exclusionist*, I consider that in Australia, for decades we have found a million reasons not to share intelligence when the consequences of taking the risk of doing so were far too great to overcome. While there has certainly been a loosening up of an earlier more conservative and rigid approach, Australia has been slow to shift policy gears in this area. In Australia we have tended to get caught up in the *need-to-know* versus the *need-to-share* doctrine. A rigid approach to intelligence exchanges that does not recognise the role and contributions of the private sector, leads to far too many incomplete pictures.

INQUIRES AND INTERNATIONAL PERSPECTIVES

The United Kingdom (UK) and the United States of America (USA), by contrast, have adopted an overarching policy position that is less risk averse than we have seen to date in Australia. The UK and the USA are more willing to take risks about sharing intelligence and more willing to share openly with the private sector. In making this comment, I draw on my experiences in conducting a number of national and international inquiries on behalf of the Australian government.

In many ways, a number of those inquiries have had at their core, the consequences of taking a traditional view of sharing intelligence and not stretching to find non-traditional links and channels for sharing intelligence. This has at times been driven by a fear on behalf of those holding intelligence of being accused of passing on information they should not and as a result, not passing it on at all. Intelligence tensions between government and policing agencies and the private sector also tend to be exacerbated when there is a failure to recognise that a traditional focus narrows the potential intelligence base which inevitably leads to incomplete intelligence pictures.

A key risk to completing the intelligence picture also comes from government and policing agencies failing to recognise that many of the large multi-national companies that own and operate key civil infrastructure in Australia, have very sophisticated intelligence arrangements within their companies. In reality, it is often these companies that have a far better overall

intelligence picture about security threats to their infrastructures than government agencies, including intelligence agencies. This is largely because many of these companies operate internationally in regions of serious piracy and threats of terrorism. Therefore, the collection and assessment of a broad spectrum of intelligence is undertaken within this private sphere to develop security plans and responses.

My own experience is that despite there being evidence of intelligence gaps, Australian policy has been slow to shift gears and recognise the value in mutual exchanges of intelligence based on trust. In reality, the risks we take from not sharing are far less than the consequences we always face in not doing so. We need to actively look for ways to share rather than reasons not to.

CHALLENGES, BENEFITS AND BARRIERS TO INTELLIGENCE SHARING

Having identified that there are significant risks of not sharing intelligence and in not taking a broad view of the intelligence base, it is necessary to look beyond the dominant policy position to examine the broader benefits and barriers to intelligence sharing.

There are clear and important differences between the operation of public intelligence agencies and private intelligence agencies. These differences arise not only because the former is taxpayer funded and the latter business and profit driven, but in the underlying business models and corporate priorities of the private sector that use the intelligence product. The business driven private sector makes them much more likely to be highly motivated, to focus on the security outcomes that will be achieved by the use of intelligence products and much more likely to minimise processes that impede sharing of intelligence.

The amount of intelligence that is shared in the private sector and between major multi-national companies that own and operate major civil infrastructures is substantial. In their day to day operating environments, there are clear pressures for any intelligence product to be valuable to the respective company in terms of its reputation, its profits, protection from industrial/economic espionage, and the potential to expand its business into new areas. These corporate priorities create an ongoing business demand for targeted intelligence product that is integrated into strategic and operational decision making. This business imperative does not often exist in government circles outside of responding to new and emerging threat.

A core challenge in Australia is the historical reticence to fully develop genuine two-way intelligence sharing between public intelligence agencies and the private sector. In my experiences, my assessment is that government agencies tend to engage with the private sector in terms of intelligence when there is a specific interest for them in doing so. In these instances, an agreement is reached and the private sector intelligence product is shared. Nevertheless, industry has been very vocal in its criticism of government agencies that this is not reciprocated. There are key challenges as well as significant benefits for this to be more strategically addressed in Australia.

In working through these challenges, a key factor will be raising the bar of mutual understanding. What has become clear to me is that government has a very incomplete level of understanding of the value to the overall intelligence picture that can be provided by private intelligence sources. As a result governments are reluctant to share intelligence. This is because governments do not have a sufficient understanding of what is potentially on offer and therefore how if properly utilised and managed through a genuine partnership, the benefits that can flow to both sectors.

In government we can get caught up with reasons for not sharing. The focus should be on what avenues there are for sharing intelligence. The challenge is to strike the balance between genuine security threats without diminishing the rights of people to go about their lawful business. What is essential is that parameters are set around what is to be collected, who will analyse it and what is done with it.

CONCLUDING REMARKS

In conclusion, it is my view that private intelligence is a fact of life and it will continue to have a role to play in Australia. With this in mind, what is essential is a better understanding of some of the differences, limitations and the inhibitors to a full exchange of intelligence between government and policing agencies and the private sector and private intelligence agencies. The challenge to current and future policing and policy leaders is to look for ways to share rather than reasons not to. It is through doing this that both sectors can be better assured of a more complete intelligence and therefore security picture.

ABOUT THE AUTHOR

Mick Palmer, AO, APM, is a distinguished law enforcement professional who has conducted sensitive governmental and corporate inquiries since his retirement as Commissioner of the Australian Federal Police in 2001. Palmer conducted a number of reviews and inquiries for both the Federal and State governments as a private consultant, including the high-profile 2005 *Cornelia Rau Report*. He took up the role of Federal Government Inspector of Transport Security in 2004. Between 2004 and 2012, Palmer headed many sensitive reviews and inquiries with many of his inquiry reports being tabled in Parliament. He stepped down from his position as Inspector of Transport Security in June 2012 and is now an Adjunct Professor at Griffith University, Queensland, Australia.

- o O o –