

Is ASIO's Corporate Governance an Oxymoron?

Mark Rix

University of Wollongong, Australia

Abstract

This paper investigates corporate governance in the Australian Security Intelligence Organisation (ASIO), Australia's domestic intelligence agency. The paper seeks to determine and understand the extent to which ASIO's approach to corporate governance emulates that of organisations in the wider public sector and the private sector. This examination of ASIO's corporate governance considers the organisation's purpose, functions and extraordinary powers focusing on the importance of secrecy to achieving its objectives. The paper will also assess whether it is appropriate to attempt to assess ASIO's corporate governance in the same terms, and according to like standards, as are used to evaluate governance in 'normal' or 'regular' public and private sector organisations. Finally, the paper provides an overall evaluation of ASIO's approach to corporate governance and considers how this approach affects the organisation's treatment of its stakeholders and the extent to which it serves their interests.¹

Key Words

Australian Security Intelligence Organisation, corporate governance, security and secrecy, oversight and accountability

Introduction

This paper investigates the question of whether corporate governance principles and practices that apply to most organisations in the private and public (and, not-for-profit) sectors are also applicable to intelligence agencies like the Australian Security Intelligence Organisation (ASIO). ASIO is Australia's domestic intelligence agency. Of course, ASIO is a part of the broader Commonwealth public sector but its functions and extraordinary powers set it well apart from agencies, departments and the like belonging to the 'regular' public sector.² These distinguishing functions and powers have a distinct tendency to make questions about the corporate governance of ASIO seem futile and on the face of it even a little absurd. Like most other aspects of ASIO, its corporate governance is a closely-guarded secret with any information and documentation that could be useful or revealing accordingly receiving a very high level of classification. The little information regarding its corporate governance that is available in the public domain is essentially part of an exercise in glib public relations including modish

Copyright © 2015 Victoria University. This document has been published as part of the Journal Law and Governance in both online and print formats. Educational and non-profit institutions are granted a non-exclusive licence to utilise this document in whole or in part for personal or classroom use without fee, provided that correct attribution and citation are made and this copyright statement is reproduced. Any other usage is prohibited without the express permission of the publisher.

references to 'outreach' and 'stakeholder satisfaction', and trite corporate branding of the 'our work', 'our values' and 'our performance' kind.³ In any event, ASIO's extraordinary powers and the extraordinary secrecy surrounding the organisation give questions about its governance, and performance in protecting Australia's national security, a great significance with

¹ ASIO is formally designated 'Australia's national security intelligence service' and, according to its website, is 'the only Australian intelligence agency which both collects and assesses security intelligence.' ASIO operates under the direction of the Director-General of Security who is directly responsible to the Commonwealth Attorney-General <www.asio.gov.au>.

² For an investigation of ASIO's functions and extraordinary powers, including the secrecy surrounding them, see M Rix, 'Security without secrecy? Counter-terrorism, ASIO and access to information', in D Baldino (Ed), *Spooked: The Truth about Intelligence in Australia*, NewSouth Publishing, Sydney, 2013, pp 240-263.

³ ASIO, Strategic Plan 2013-16, pp 1-4 <www.asio.gov.au/Publications/Strategic-Plan.html>.

an urgent need for convincing answers. Naturally, this does not entail that these questions will be at all easy to answer. But, it does mean that it is nevertheless important to ask them and seek whatever answers are able to be uncovered. It is pretty obvious that reaching any understanding of ASIO governance requires some knowledge of the organisation's purpose and powers and the importance of secrecy in the performance of its mission and exercise of its powers. Left open is the question of how in any case its performance in protecting national security is to be evaluated when its operations are shrouded in secrecy and underwritten by legislation that protects this secrecy. The legislation imposes harsh penalties for, amongst other things, unauthorised disclosure of information regarding ASIO's operations, the identity of ASIO employees or 'affiliates', and the detention and questioning of suspects *and* non-suspects while they are held in detention and for some time afterwards. This raises a potentially intractable obstacle for an investigation of ASIO corporate governance: secrecy could well be a necessary, if not altogether sufficient, condition of ASIO undertaking its mission to protect Australia's national security. It is a moot point whether secrecy makes it impossible to know whether this is or is not the case. However, assuming for the moment secrecy *is* a necessary condition of ASIO performance then it follows that if ASIO and its activities were not shrouded in a thick blanket of secrecy then it couldn't even begin to set about protecting Australia's national security which is its overriding purpose. It would fall at the first hurdle because on this score at least openness and transparency would prevent it from undertaking almost any effective activities or operations towards achieving this purpose and therefore completely undermine its performance. And, if secrecy is necessary for ASIO's successful performance in protecting national security, this would effectively put a definitive stop to any attempt to evaluate its performance, and the governance arrangements behind it, in a meaningful and informative way for to do so would be utterly futile and ultimately fruitless. Paradoxically, of course, secrecy makes such a conclusion an almost completely unfounded one. This is also the case with the opposite or any other conclusions.

This paper is based on the premise that an effective, comprehensive approach to or system of corporate governance is essential for high-performing, responsive and ethical organisations in both the private and public sectors. Such a corporate governance approach or system would at a minimum embody high standards of leadership and management including disclosure, transparency and accountability, complementary principles underpinning and governing the performance of staff and how they conduct their operations, and an overall culture of integrity, decency, ethical conduct, responsibility, and accountability. In addition to these values, principles and practices, effective corporate governance requires a genuine commitment from an organisation and its leaders, managers and staff to openness and honesty, transparency and disclosure. These should be the values at the core of an organisation's culture. Much more could of course be said about what else comprehensive corporate governance entails, including sound risk management policies, an effective whistleblower policy with assured whistleblower protections, a real commitment to corporate social responsibility, and a sincere, respectful engagement with stakeholders and dedication to serving their interests. But the point here has simply been to establish the underlying principles, values and practices which together comprise robust and comprehensive corporate governance for almost any organisation from either the private or the public sector. Armed with these insights into what corporate governance is and should be, the paper investigates corporate governance in ASIO seeking to determine and understand the extent to which its approach or system emulates that of its counterparts in the private and public sector.

Examining early conceptions of corporate governance, the next section provides an overview of the principles and practices that underpin corporate governance and argues that the stakeholder model or theory is, despite its shortcomings and with insights drawn from enlightened shareholder theory, one of the more useful amongst a range of alternative theories for investigating and understanding corporate governance ASIO-style. The following section investigates corporate governance in ASIO examining ASIO's mission, functions and powers with a focus on the importance of secrecy to the effective performance and successful achievement of its mission to protect Australia's national security. Included here is an assessment of ASIO's response to the Snowden disclosures. Then, an investigation of ASIO's oversight and accountability framework is undertaken evaluating how secrecy affects the framework's effectiveness. The concluding section provides an overall evaluation of ASIO's approach to corporate governance and considers how this approach affects the organisation's treatment of its stakeholders and

how well it serves their interests. This is of considerable interest and concern because ASIO's most important stakeholders are the Australian people including *their* security and the rights and freedoms it is claimed that they have and should be able to enjoy. This assessment of ASIO's governance will briefly consider whether secrecy contributes to or detracts from its performance in protecting national security so that these stakeholders are able to exercise and enjoy their freedoms and rights.

Corporate governance: principles and practices

The importance of the theory and practice, discipline or subject, of corporate governance is captured in this enduring and influential definition:

Corporate Governance is concerned with holding the balance between economic and social goals and between individual and communal goals. The corporate governance framework is there to encourage the efficient use of resources and equally to require accountability for the stewardship of those resources. The aim is to align as nearly as possible the interests of individuals, corporations and society.⁴

Cadbury extends this definition by asserting that disclosure is the foundation of any system of corporate governance because it is this which is the 'basis of public confidence in the corporate system'. In his view, corporate governance is also based on the principles of transparency, accountability, fairness and responsibility which are all 'universal in application'.⁵

It is certainly clear that, for Cadbury, corporate governance is not simply about maximising shareholder value but with maintaining a balance between often inconsistent economic and social, individual and communal goals and with reconciling to the extent possible the competing interests of different stakeholder groups. The corporate governance system should not only promote the efficient use of resources but also hold corporations, their owners and those who lead and direct them responsible and accountable for how well resources are managed. Thus, sustainability and corporate social and environmental responsibility, and ethical business practice are also consistent with, if not core components of, Cadbury's conception of corporate governance. It should be equally clear that his conception is highly applicable to corporate governance in the public and not-for-profit sectors where key stakeholders whether they are called voters, taxpayers, citizens or members take the place of and in many respects have similar rights and responsibilities to the shareholders of publicly-listed companies.

Writing at about the same time as Cadbury Brian Cheffins, SJ Berwin Professor of Corporate Law at Cambridge University, observed that the discipline or subject of corporate governance 'draws from a variety of fields other than law, including economics, ethics, accounting and finance' and that understanding the issues involves therefore requires students (and practitioners) to acquire 'some familiarity with the concepts, assumptions and vocabulary of these various disciplines'.⁶ Studying, and indeed practising, corporate governance should accordingly be based on an awareness and understanding of the economic, political, social and cultural context within which publicly-listed companies and other organisations operate. And, in an early account of the continuing debate about whether shareholder value or stakeholder interests should take precedence in corporate governance regimes, Cheffins also noted that 'whereas some prefer to confine discussion by focusing on ways to improve the return shareholders receive, others treat all corporate stakeholders, including employees, suppliers, customers and even society at large, as being part of the corporate governance equation'.⁷ While it is obvious that Cheffins was especially concerned with the governance of publicly-listed companies his conception of corporate governance is, like Cadbury's, readily applicable to the corporate governance of public sector organisations and non-profits.

⁴ Sir Adrian Cadbury, Foreword, MR Iskander & N Chamlou, *Corporate Governance: A Framework for Implementation*, World Bank Group, Washington DC, 2000, p vi. Sir Cadbury, formerly Chairman of the famous chocolate family's firm and later of Cadbury Schweppes, has long been a strong advocate of the importance of corporate governance and of meaningful corporate governance reform. In 1991, he was appointed Chair of the UK Committee on the Financial Aspects of Corporate Governance which in 1992 produced the Cadbury Report and Code of Best Practice.

⁵ Cadbury, above n 5, at p v.

⁶ BR Cheffins 'Teaching Corporate Governance' (1999) *Legal Studies* 19 515 at 520.

⁷ Cheffins, above n 7, at 524-525.

It is clear from the comments of Cadbury and Cheffins that what has become variously known as the stakeholder model, theory or philosophy of corporate governance has had a long and significant influence on the development of the subject or discipline of governance and on governance practice. As suggested above, this enduring influence has helped to ensure that corporate social and environmental responsibility and ethical business practice evolved as key principles and aspects of both governance theory and practice. Advocates of stakeholder theory contend as Cheffins suggested that directors and the corporations they oversee are responsible and accountable to a range of stakeholders other than shareholders, the many groups and individuals affected by their decisions, behaviour and operations. Responsibility and accountability are or should be ‘the price society demands for the privilege of incorporation, granting shareholders limited liability for the company’s debts.’⁸ One of the main difficulties encountered by advocates of stakeholder theory is in deciding how to balance the often competing interests of different stakeholder groups when it is almost always impossible to maximise or at least adequately satisfy all stakeholder interests at the same time.⁹ A key question emerges from this difficulty focusing on director and management accountability: in seeking to serve the interests of different stakeholders, whose interests should be given priority and how can directors and managers be held accountable for favouring certain stakeholder interests over others? This also leaves unanswered a similarly awkward question about how director and management performance should be evaluated and rewarded. As Bob Tricker suggests, enlightened shareholder theory (or, enlightened shareholder value)—a sort of hybrid of stewardship theory and stakeholder theory—can go some of the way in resolving these dilemmas. The theory acknowledges that over the longer term shareholder value can be increased or sustained only by satisfying the interests of key stakeholders.¹⁰ The practical application of enlightened shareholder theory is not without its own difficulties and challenges but it is beyond the remit of this paper to explore these any further.

Despite its evident shortcomings, stakeholder theory continues to be influential in the development of corporate governance theory and practice. This influence is a product of its insistence that corporate directors have important responsibilities and accountabilities beyond simply serving the interests of shareholders by creating and increasing long-term profitability and wealth. The notion of corporate social (and, environmental) responsibility and the kindred ‘ethical business practice’ have both grown out of this recognition. In taking their broader responsibilities and accountabilities seriously, and modifying their behaviour and operations in accordance with these, directors and corporations can be granted what is widely referred to as a ‘social licence to operate’. For John Morrison, Executive Director of the Institute of Human Rights and Business, the ‘social licence’ concept is even more important and useful than that of ‘corporate social responsibility’ which can be perfunctory, self-serving and little more than an exercise in reputation management and brand enhancement. Because business can never award itself a ‘social licence’, being given such a licence by affected communities and constituencies requires that business activities and operations enjoy ‘sufficient trust and legitimacy, and [have] the consent of those affected.’ In managing social, environmental, political and legal risks, businesses can’t by themselves decide how much prevention, deterrence or mitigation is sufficient. Stakeholders and other rights-holders should be involved in setting ‘thresholds of due diligence’ (in other words, audit, oversight and accountability mechanisms) even if these have already been determined in relevant legislation. Otherwise, such thresholds or standards can lack the legitimacy required for social permission to be granted making it difficult for business to proceed with planned operations and activities.¹¹ Clearly then, companies cannot exert anything like complete control over ‘social licence’ but they can nevertheless manage ‘issues such as transparency, accountability, clarity about benefits, remedies and adequate due diligence’.¹² Again, these are the conditions that have to be satisfied before social consent or permission is granted in the first place.

⁸ B Tricker, *Corporate Governance: Principles, Policies and Practices* (2nd ed), Oxford University Press, 2012, p 70.

⁹ Christine A Mallin, *Corporate Governance* (4th ed), Oxford University Press, 2013, p 20.

¹⁰ Tricker, above n 9, at 74.

¹¹ John Morrison, ‘Business and Society: Defining the “Social Licence”’, *The Guardian* (2014) 29 September <<http://www.theguardian.com/sustainable-business/2014/sep/29/social-licence-operate-shell-bp-business-leaders>>. See also Jason Prno, D Scott Slocombe, ‘Exploring the origins of “social license to operate” in the mining sector: Perspectives from governance and sustainability theories’, *Resources Policy* (2012) 37 346.

¹² Morrison, above n 12.

As Cadbury asserted long ago, disclosure is a founding principle of corporate governance because this is the basis of public confidence in business and, he might have added, in government as well. Disclosure is closely aligned with, and is complementary to, the principles of transparency, accountability, fairness and responsibility. Thus, these ancillary principles too not only apply to the governance of corporations and the ‘corporate system’ more generally, they are just as applicable to the governance of government and of the public sector including the various departments, agencies and authorities comprising it. This leaves a very large question over the meaning of governance for an agency like ASIO for which disclosure is in many respects an anathema. But, if secrecy *is* essential to ASIO’s performance in protecting the security of the country and its people then it arguably would make little sense to judge its governance, even if this were possible, by the same standards of disclosure, transparency and the like as are used in judging corporations’ and ‘regular’ public sector agencies’ governance. Accordingly, in the following sections ASIO corporate governance will be investigated beginning with an examination of its mission, values and functions, and powers with a view to determining how important secrecy is to the performance of its mission. It will also consider the critical assessment of Edward Snowden’s disclosures included in the ASIO Report to Parliament 2013-2014 and in recent speeches and addresses by ASIO officials. This is important because ASIO’s critique of Snowden clearly reveals its attitude to secrecy and disclosure which has significant implications for how well it serves the interests of its key stakeholders. An examination of ASIO’s oversight and accountability framework is then undertaken assessing how secrecy affects the framework’s effectiveness. Finally, an overall evaluation is provided of ASIO’s performance in serving the interests of its stakeholders, in particular, the Australian public.

ASIO corporate governance: security and secrecy

First, it is important to understand the meaning of security that it is ASIO’s role to protect. This is contained in Section 4 of the ASIO Act 1979 where security is defined as meaning the protection of Australia and Australians from espionage, sabotage, politically motivated violence and the promotion of communal violence, attacks on the country’s ‘defence system, foreign interference, whether these are ‘directed from, or committed within, Australia or not’ and, serious threats to the integrity of Australia’s borders and territory. This is broadened considerably by the inclusion in the definition of security of ‘the carrying out of Australia’s responsibilities to any foreign country’ in relation to any of these matters.¹³ This expansive view of security and ASIO’s role in protecting it is important background for understanding the organisation’s vision, mission, objectives and so on.

The ASIO Strategic Plan 2013-16 provides a brief and relatively accessible introduction to ASIO’s vision and mission, objectives and values (there is not the scope here to consider ASIO’s goals which in any event support its mission¹⁴). ASIO’s vision, ‘The Intelligence Edge for a Secure Australia’, is so vacuous as to warrant no further attention. Its mission is ‘To identify and investigate threats to security and provide advice to protect Australia, its people and its interests’. In other words, ASIO’s mission is the protection of Australia’s national security by collecting and assessing security intelligence and providing appropriate advice to government. ASIO’s values are unexceptionable if not also a little vacuous: Excellence, producing useful and timely advice, showing solid leadership and being professional, being innovative and improving through learning; Integrity, being ethical and unbiased, maintaining confidentiality and secrecy, respecting diversity; Accountability, being responsible in conducting operations and for outcomes, and being accountable to the Australian public through the government and parliament; Cooperation, developing a common purpose and mutual support; using appropriate communications in all relationships; having productive partnerships.¹⁵ More important than ASIO’s vision, mission and values for an understanding of ASIO’s governance arrangements are its objectives.

¹³ ASIO Act 1979, Section 4. The recent addition of border and territorial integrity to the list of threats to national security reflects the current Government’s obsession with asylum seekers and the punishment of them. <www.comlaw.gov.au/Details/C2013C00437> .

¹⁴ ASIO Strategic Plan 2013-16, above, n 4, at 3.

¹⁵ ASIO Strategic Plan 2013-16, above n 4, at 4. Some of the Strategic Plan’s text regarding ASIO’s values has been paraphrased and slightly abridged. Oddly, the Strategic Plan does not include ‘Respect, We show respect in our dealings with others’, as one of ASIO’s values unlike the Report to Parliament 2013-2014 which does so. This could have been the result of a formatting issue and, after all, they’re only words.

Under the 'Our Work' heading, the Strategic Plan makes it relatively clear, and not surprisingly, that ASIO's objectives complement and support the Government's national security strategy. There are four broad objectives of the strategy: ensuring the safety and resilience of the population as a whole; protecting and strengthening Australia's sovereignty including independence of its decision making and authority over its territory and resources; securing Australia's assets, infrastructure and institutions, e.g. supply chains, intellectual property, information technologies and communications networks, natural wealth; and, promoting a favourable international environment through influencing and shaping the country's regional and global environment so that it is conducive to Australia's interests and values.¹⁶

ASIO's objectives (and goals) are largely reflected in the Outcomes and Deliverables that are outlined in Part 2 Program Performance of the Annual Report 2013-2014. Part 2 is based on publicly-available information. There is one outcome, Outcome 1, which is 'To protect Australia, its people and its interests from threats to security through intelligence collection, assessment and advice to government.' The Annual Report lists four program deliverables: 1. security intelligence analysis and advice such as strategic and counter-espionage threat assessment and advice, border security, engaging with and advising industry groups, supporting prosecutions and litigation involving security intelligence; 2. protective security advice which includes counter-terrorism checking, personnel and physical security, and contributions to policy development; 3. security intelligence investigations and capabilities which involves maintaining and enhancing collection of 'all-source' security intelligence, analysis of complex tactical and technical data, technical R&D; counter-terrorism response, liaising with national and international partners and stakeholders, and policy development; 4 collecting foreign intelligence in Australia when requested by the Ministers of Foreign Affairs and Defence or 'incidentally' as a result of existing security intelligence capabilities or liaising with foreign partners.¹⁷ Part 2 of the Annual Report also contains a self-assessment of ASIO's performance against its two key performance indicators and in terms of each deliverable. The first of the KPIs deals with how in the reporting period ASIO's action and advice contributed to the management and reduction of risk to people and property, public, private and national infrastructure and any special events of national or international significance during the reporting period. The second deals with the security of ASIO'S activities. Clearly, then, ASIO performance against the second of its KPIs depends heavily on secrecy and the protection of secrecy. The importance of secrecy for ASIO performance against Outcome 1, and the two KPIs and each of the deliverables, is demonstrated in the Annual Report Part 3 Outcomes and highlights. This is 'a detailed report of ASIO performance and operations' against Outcome 1. Unfortunately for transparency and disclosure, and public confidence, 'This part contains a national security classification of Top Secret and is excised by the Attorney-General in its entirety...as unauthorised disclosure could reasonably be expected to cause exceptionally grave damage to the security of the Australian Government.'¹⁸ At the beginning of Part 3 it is made clear that excising Part 3 (Exclusion) was done after the Attorney-General obtained advice from the Director-General of Security that it 'is necessary in order to avoid prejudice to security.'¹⁹ No mention is made here of 'exceptionally grave damage'.

The Report's revealing critique of Snowden's revelations is contained in Part 1 The Security Environment and Outlook under the unsettling heading Espionage and clandestine foreign interference. It begins: 'Self-motivated individuals who exploit their privileged access to government information to make unauthorised disclosures of classified or other privileged information have always been a potential source of harm to Australia's interests.'²⁰ The harm that such individuals can cause has been, according to the Report, 'greatly increased by modern information technology, which allows large amounts of information to be aggregated and copied' and further 'amplified' by the internet with its capacity for easy distribution of the information to a large audience that is ready to 'consume' it. Overlooked here, and cynically inverted, was what the Snowden disclosures actually revealed: the significant harm to

¹⁶ ASIO, Strategic Plan 2013-16, above n 4, at 4. The objectives, deliverables and KPIs have all been paraphrased and slightly abbreviated.

¹⁷ ASIO Report to Parliament 2013-2014, pp 12-13 <www.asio.gov.au/Publications/Report-to-Parliament/Report-to-Parliament.html>.

¹⁸ ASIO Report to Parliament 2013-2014, above n 18, p xiv.

¹⁹ ASIO Report to Parliament 2013-2014, above n 18, p 37.

²⁰ ASIO Report to Parliament 2013-2014, above n 18, p 7.

human rights and democratic freedoms increased by modern information technology allowing the bulk collection and aggregation (storage and retention) of large amounts of information that has been amplified by the internet making it even easier for agencies like the US NSA, UK GCHQ and Australian ASD to collect, aggregate and cross-reference vast amounts of information about the private communications (metadata and content) of innocent individuals. In any event, for ASIO Snowden was a 'malicious insider' who caused 'wide-scale and indiscriminate' harm that will be 'felt for many years' to come because his actions have the 'very real potential' to 'inspire and influence people who wrongly regard him as a whistleblower'.²¹ In substantiating its claim that it is incorrect to regard Edward Snowden as a real whistleblower, the Report quotes at length from Attorney-General George Brandis' speech to the Centre for Strategic and International Studies in Washington DC delivered in April 2014. In this speech, Brandis cited *The Snowden Operation* by Edward Lucas (Lucas is *The Economist's* Senior Editor), who in turn had cited Princeton University academic Rahul Sagur's *Secrets and Leaks*. Based on these sources, Brandis was able to assert that there are three principal criteria that have to be satisfied for a person to qualify as a whistleblower: the person must have unambiguous and compelling evidence of abuse, misconduct or corruption; disclosing the information must not disproportionately threaten public safety; and, to the extent possible, the scope and scale of the information 'leaked' must be limited. According to Brandis citing Lucas, Snowden failed the whistleblower test on all three counts.²²

The Snowden exposures, disclosures or 'leaks' have ensured that the issue of what is, and what is not, whistleblowing and who should be, and who should not be, regarded as a whistleblower, is now a thorny and vexed one for ASIO. Snowden's actions have also reinforced for ASIO the need for greater secrecy and the strict protection of secrecy. In his Review which precedes the ASIO Report proper, then Director-General of Security David Irvine acknowledges that effective disclosure (whistleblowing) laws ensure that (undefined) 'improper conduct' within government including its intelligence agencies 'is investigated and dealt with'. Thus, ASIO, and its Director-General, welcomed the enactment of the Public Interest Disclosure Act 2013 which commenced in 2014. However, it did so not because this Act provides for adequate protections for genuine whistleblowers who expose misconduct, abuse of powers or corruption but because the Act contains measures for the 'appropriate protection against the unauthorised disclosure of intelligence information' by people like Snowden who are 'self-motivated malicious insiders' frequently acting out of a personal grievance or misguided agenda.²³ In other words, Irvine and ASIO welcomed the introduction of the Public Interest Disclosure Act precisely because the Act protects the secrecy of the organisation, its operatives and its operations from unwanted exposure by even genuine whistleblowers and journalists who act in the public interest. In any event, investigating the actions of people like Snowden is 'complex, resource-intensive and highly sensitive' requiring ASIO and similar organisations to be 'appropriate and proportionate' in their response balancing 'individual privacy considerations' against the potential harm these individuals can inflict by their actions.²⁴

Some of the same themes were taken up by one of the two (anonymous) Deputy Directors-General of Security who addressed the Security in Government Conference in September 2014.²⁵ In keeping with the Conference theme, the Deputy Director General's address was titled 'The espionage threat from trusted insiders'.²⁶ According to the Deputy Director-General, it is not only malicious insiders recruited

²¹ ASIO, Report to Parliament 2013-2014, above n 18, at 7.

²² ASIO Report to Parliament 2013-2014, above n 18, at 7. It is telling that Brandis did not here quote the meaning of 'public interest disclosure', and provisions for protection of disclosers, contained in the Public Interest Disclosure Act 2013 Subdivision A and Subdivision C, of Division 2 Part 2.

²³ Director General's Review in ASIO Report to Parliament 2013-2014, above n 18, at ix.

²⁴ ASIO Report to Parliament 2013-2014, above n 18, at 7.

²⁵ According to the Attorney-General's Department website, the Conference is hosted by the Department's National Security Resilience Policy Division, has been a regular event since 1987 and enables 'security agency advisers [to focus] on protective security issues.' The 2014 Conference theme was 'Mitigating the trusted insider threat'. ASIO provided a separate briefing to the conference on the Australian security environment and trends in protective security countermeasures. However this 'was open to Australian Government employees only with a current security clearance at the Negative Vetting Level 1 (SECRET level) or above.' <www.ag.gov.au/NationalSecurity/SecurityGovernmentConference/Pages/Security-in-Government-Conference-2014.aspx> .

²⁶ Deputy Director-General of Security, 'The Espionage Threat from Trusted Insiders'. Address to the Security in Government Conference 2014, 2 September <www.asio.gov.au/Publications/Speeches-and-Statements/Speeches-and-

by foreign intelligence services who pose a significant risk to national security and potentially cause ‘catastrophic harm’ to Australia and its interests. Just as harmful are ‘self-motivated malicious insiders’ motivated by ‘disgruntlement, revenge, ego, a sense of the misguided greater good or loyalties, or financial gain’ who ‘betray the trust of their employer’. Like his boss David Irvine, the Deputy Director-General had Edward Snowden squarely in his sights. She/he quoted the Attorney-General to reject the claim that Snowden is a whistleblower but also to label him a ‘traitor’: ‘He is a traitor because, by a cold-blooded and calculated act, he attacked your country [the US] by significantly damaging its capacity to defend itself from its enemies, and in doing so, he put your citizen’s [*sic*] lives at risk. And, in the course of doing so, he also compromised the national security of America’s closest allies, including Australia’s.’²⁷

In the end, according to the Deputy Director-General, the Government and public servants have a ‘fundamental duty’ to uphold and defend the country’s interests including ‘holding secrets’ and to protect such confidential (that is, classified) information ‘in many instances for life’.²⁸ His then boss, David Irvine, had had a similar message when in August 2014 he addressed the National Press Club (an extremely rare event for a Director-General) and delivered a speech titled ‘Diligence in the shadows—ASIO’S responsibility’. Spruiking ASIO’s role and work, Irvine pointed out that the former is identifying and assessing threats to national security and to the lives and safety of Australians while the latter, which is ‘predictive and advisory’, is essentially an exercise in risk management which enables the Government to take preventative measures. As well as being different from the law enforcement work of police services, another ‘defining characteristic’ of ASIO’s work is the ‘need for a security intelligence service to operate in secrecy’.²⁹ In explaining why secrecy is necessary, and in another cynical allusion, Irvine noted that ‘As any journalist will understand, we need to protect our sources’ (community contacts or covert human sources) from being put in ‘real personal danger’.³⁰ In addition, not only did secrecy protect ASIO’s ‘operational techniques’ from becoming known to ‘our adversaries’ who if they had this knowledge would be better placed to disguise their ‘malicious activities’, it also protected from exposure any intelligence provided by ‘our friends and allies’. Irvine’s final apologia for secrecy is that bizarrely it is ‘to the benefit of individuals whom ASIO may be investigating’ because ‘[t]he reputations, livelihoods and future prospects of such people, *many of whom may turn out not to be of security concern after all*, may be damaged if our work is not conducted discreetly, out of the public gaze.’³¹

The all-encompassing definition of security contained in the ASIO Act is matched by the all-encompassing secrecy surrounding ASIO, its operatives and operations. The ASIO Act, the National Security Information (Criminal and Civil Proceedings) Act 2004 and, ironically, the Public Interest Disclosure Act 2013 all work in concert having ‘the effect of creating a sort of three-sided hall of mirrors in which each Act’s restrictions on the disclosure, and availability, of information are tightened as one Act reinforces the others in providing fewer and narrower avenues for access to and release of information in the conduct of terrorism investigations and any subsequent trials.’³² The Acts’ severe restrictions on disclosure of and access to information about ASIO and its activities have been further tightened and reinforced by provisions contained in the National Security Legislation Amendment Act (No. 1) 2014. This Act creates an offence with a prison sentence of up to five years and an aggravated offence (where a discloser intentionally or recklessly endangers the health and safety of a person or adversely affects the conduct of an SIO) with a maximum penalty of 10 years imprisonment for the unauthorised disclosure of information about ASIO special intelligence operations (SIOs). An SIO is

Statements/DDG-Speech-02-September-2014.html>. It is a moot point whether the Deputy Director-General’s speech was in fact ASIO’s ‘separate briefing’ to the conference.

²⁷ George Brandis cited in Deputy Director-General of Security, above n 27.

²⁸ ASIO Report to Parliament 2013-2014, above n 18, at 7.

²⁹ Director-General’s Speech to the National Press Club, 27 August 2014. In support of ASIO secrecy, Irvine cited the Royal Commission on Intelligence and Security [Hope Royal Commission], Fourth Report, Volume 1 [ASIO], published in 1977/78: ‘Intelligence agencies simply cannot operate in full public view if they are to be effective.’

<www.asio.gov.au/publications/speeches-and-statements/speeches-and-statements/dgs-speech-27-august-2014.html>.

³⁰ Director-General’s Speech, above n 30.

³¹ Director-General’s Speech, above n 30 (emphasis added).

³² Rix, above n 3, at 245.

defined as an ASIO operation that is relevant to its performing a ‘special intelligence function’ which includes collection and analysis of intelligence related to security. No allowance is made for public interest disclosures and whistleblowing by ASIO employees or of disclosures by journalists. The offences therefore seriously encroach on free speech and expression and on media freedom.³³ In addition to these restrictions, the National Security Legislation Amendment Act enhances ASIO’s surveillance powers by strengthening its powers to collect and retain metadata.³⁴ These enhancements are complemented by the additional powers handed to ASIO in the Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014 which enables ASIO to collect and retain metadata and to obtain access to computers even when these have nothing to do with the protection of national security.

ASIO corporate governance: oversight and accountability?

According to the Strategic Plan 2013-16, ‘Our [ASIO’s] corporate governance arrangements support the management and evaluation of performance across a range of ASIO’s functions.’³⁵ The Strategic Plan itself is an important component of these governance arrangements reflecting ASIO’s responsibility not only for meeting Australia’s current security needs but also for ‘ensuring that Australia’s national security capability is maintained’ to enable it to meet the country’s future security challenges.³⁶ The Plan underpins ASIO’s strategic and operational planning and sets the organisation’s overall direction in business plans, the priorities of its corporate committees, and ‘executive focus’. It also ensures that ASIO’s investments in capability development are aligned with the goals in the Strategic Plan and that its performance is measured and reported in accordance with the Plan. The Strategic Plan also briefly outlines ASIO’s oversight and accountability framework. This framework is explained in a little more detail in the Director-General’s speech to the National Press Club and more detail is provided in the Report to Parliament and other ASIO documents.

In his speech, the Director-General pointed out that

ASIO is accountable directly to the Parliament. The Organisation provides an annual report to the Parliament of its activities, has its activities scrutinised at Senate Estimates [Committee], it briefs the Opposition, appears before the bipartisan Parliamentary Joint Committee on Intelligence and Security, and provides as required public and private briefings to various Senate committees. It is audited by the ANAO [Australian National Audit Office].³⁷

In addition to these arrangements, ASIO’s oversight and accountability framework contains a number of other important components. ASIO reports yearly to the National Security Committee of the Cabinet and submits a classified annual report to Parliament. The Attorney-General has oversight of all ASIO operations and issues each warrant for the use of ASIO’s ‘intrusive powers.’ The ASIO Act requires the organisation to comply with the Attorney-General’s Guidelines for performing its functions of collecting, correlating, analysing and communicating intelligence related to security and in relation to politically motivated violence.³⁸ ASIO’s security assessments can be reviewed by the Administrative

³³ M Biddington ‘National Security Legislation Amendment Bill (No. 1)’ (2014) *Bills Digest*, 19 1 at 29 <<http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fbillsdgs%2F3361366%22>>; Australian Human Rights Commission Inquiry into the National Security Legislation Amendment Bill (No. 1). Submission to the Parliamentary Joint Committee on Intelligence and Security (2014) at 14 <www.humanrights.gov.au/submissions/submission-inquiry-national-security-legislation-amendment-bill-no-1-2014>

³⁴ Australian Human Rights Commission, above n 34, at 10; Biddington, above n 34, at 13.

³⁵ ASIO Strategic Plan 2013-16, above n 4, at 4.

³⁶ ASIO Report to Parliament 2013-2014, above n 18, at 60. Part 5 Corporate Management describes the role of ASIO’s various governance committees and has sections dealing with its ‘Outreach’ initiatives, ‘People’, Property, and Financial services.

³⁷ Director-General’s Speech to the National Press Club, above n 30. It should be noted that the PJCIS does not have oversight of ASIO’s operations and does not have the power to initiate its own inquiries. For more on the oversight and accountability framework see ASIO Report to Parliament 2013-2014 Part 4 ASIO and Accountability, above n 18. Also, see Senator John Faulkner’s recommendations for, amongst other things, bolstering the investigative powers of the PJCIS: J Faulkner, ‘Surveillance, Intelligence and Accountability’, 24 October 2014 <www.senatorjohnfaulkner.com.au/file.php?file=/news/TGRUOSECRG/index.html>.

³⁸ Attorney-General’s Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence) <www.asio.gov.au/About-ASIO/Oversight-and-Accountability/Attorney-General-Guidelines.html>.

Appeals Tribunal, the Independent Reviewer of Adverse Security Assessments and the courts. The Independent National Security Legislation Monitor reviews the legislative framework within which ASIO carries out its counter-terrorism work and can recommend changes to legislation. The legality, propriety and proportionality of ASIO's work are subject to independent oversight by the Inspector-General of Security and Intelligence, the peak oversight and accountability for Australia's various intelligence services. The role of the IGIS is to ensure that the intelligence services, including ASIO, act legally and with propriety and in accordance with ministerial guidelines and directives, and with respect for human rights. The IGIS has wide-ranging powers including those of a Royal Commission. Among the IGIS's specific powers are conducting inquiries into the activities of the intelligence agencies from the IGIS's own motion or in response to a reference or complaint from the responsible Minister, requiring witnesses to attend inquiries conducted by the Inspector-General, and taking sworn evidence and copying and retaining documents. Inspector-General staff are also able to enter security agency premises when conducting an inquiry and act on complaints from ASIO and ASIS employees about certain matters relating to the conditions of their employment.³⁹

The Director-General regards this oversight and accountability framework as 'robust and effective'. However, his view is not a universally shared one. In mid-October 2014, for example, the Office of the Inspector-General of Intelligence and Security began recruitment of five more staff to add to the existing 12 in order to enable the office to monitor ASIO's exercise of the enhanced powers it was granted by the two amendment bills that were considered above.⁴⁰ A number of commentators were concerned about the extent to which five additional staff would actually strengthen the Office's capabilities to provide thorough oversight of ASIO, as well as of the other intelligence agencies such as the Australian Secret Intelligence Service (ASIS, Australia's overseas secret intelligence collection agency). Professor George Williams of the Gilbert + Tobin Centre of Public Law at UNSW pointed out that 'it has been regarded for some time that IGIS is underfunded and has not kept up with the enormous increase of personnel within the intelligence community and the significant expansion of their powers.' Matthew Rimmer, of the ANU College of Law, agreed with Williams calling the IGIS 'a bit of a paper tiger' that provides only 'weak oversight'.⁴¹ Independent Senator Nick Xenophon also expressed criticism of the Inspector-General. Commenting on the Inspector-General's inquiry into a case involving an Australian soldier who allegedly pulled a gun on an ASIS agent, Senator Xenophon noted that she seemed to have a 'very cosy and collegial relationship' with ASIS and the other intelligence agencies 'which is not appropriate'. He also believed that in investigating the incident, the Inspector-General had been 'either misled or lied to'.⁴² Under the existing legislative framework, lying to the Inspector-General by an intelligence service carries no penalty.

Conclusion: Public confidence and social licence by default?

In spite of the Director-General's assurances, ASIO lacks a comprehensive and robust oversight and accountability framework. The oversight bodies are hamstrung by legislation protecting the secrecy shrouding the organisation and its operations including by imposing limits on the powers of the oversight bodies themselves. And, because when it is claimed that national security is at stake the oversight bodies seem reluctant to exercise to the extent possible the limited powers that they already have. The relevant legislation, including the misnamed Public Interest Disclosure Act 2013, also severely penalises genuine whistleblowers and journalists from making disclosures about ASIO and its operations even if these disclosures are in the public interest. These tight restrictions on the availability of and access to information about ASIO have been reinforced and further tightened in the National Security Legislation Amendment Act (No. 1) 2014. If as Cadbury asserted, disclosure is the foundation of corporate governance because without disclosure the public cannot have confidence organisations are being run

³⁹ Roles and Functions of the Inspector-General <<http://www.igis.gov.au/about/index.cfm>> .

⁴⁰ H Belot, 'Inspector-General of Intelligence and Security launches recruitment drive to monitor ASIO', *The Sydney Morning Herald*, 13 October 2014. The current Inspector-General is Dr Vivien Thom.

⁴¹ Williams and Rimmer cited in H Belot, 'Intelligence watchdog's oversight called "weak" as new powers granted to spy agencies', *The Sydney Morning Herald*, 14 October 2014.

⁴² Chris Uhlmann, 'Nick Xenophon criticises ASIS handling of incident', ABC News, 21 October 2014 <www.abc.net.au/new/2014-10-21/nick-xenophon-criticises-asis-handling-of-incident/5289014>.

effectively and in the interests of genuine stakeholders then there are few grounds for the Australian public to have much confidence that ASIO is serving their interests or for giving it a *carte blanche* social licence. On this score at least, ASIO's corporate governance *is* an oxymoron. In the end, however, this dilemma is an unresolvable one for it cannot be concluded with any certainty that national security is only able to be protected with tight secrecy. Tight secrecy, and a lack of transparency and accountability accompanying it, comes with considerable risk of misuse and abuse of power and limits on the Australian people's ability to enjoy their fundamental rights and freedoms.

