Author: Paul Hubbard, University of Tasmania
Private Bag 89 Hobart Tasmania 7001
phubbard@utas.edu.au

Title: Freedom of Information and Security Intelligence: An economic analysis in an Australian context

Volume 1 issue 3

Abstract

Australian discussions of information policy broadly accept the assumption that secrecy is necessary when national security is concerned. Despite greater transparency in other areas of information law, security and defence information has remained off limits to critical review. Australian intelligence agencies are not subject to the Australian Freedom of Information Act, and there is a low-threshold exclusion for defence and security related information.

The underlying assumption that secrecy is necessary and desirable can be challenged by applying concepts from information economics. Although some information asymmetry is unavoidable, Joseph Stiglitz has warned of inefficient rent-seeking which follows. Too much secrecy not only undermines democratic oversight, but also undermines the efficiency and effectiveness of national security processes. Moreover, these processes were designed for a cold-war world where information was a scarce resource.

As with other areas of government, greater transparency can lead to better outcomes in national security. Citizens can directly engage in the policy process, and may even be directly empowered to take direct action. The argument against transparency, that information may be used maliciously in the wrong hands, will only be the case in limited circumstances. The work of Peter Swire provides us with a basic calculus to determine when transparency will help, and when it will hinder security. This approach provides more coherent information policy and more effective national security.

The current Australian approach to security information is unsophisticated. There is an assumption that secrecy is necessary to protect national security, and given the importance of Australia's national security, secrecy in the name of national defence must trump the citizen's right of access under freedom of information legislation. However, if we are to have a coherent approach to information law in Australia, it is necessary to reject the trump card approach, in favour of an approach which balances competing and legitimate information rights. This relationship between security and the Australian *Freedom of Information Act* is addressed in Part 1.

Part 2 applies the insights of economist Professor Joseph Stiglitz to information asymmetries in order to view national security information in terms of information flow. It accepts that some degree of information asymmetry is both necessary and desirable. But information asymmetries, in the form of secrets, also create inefficiency and damage accountability. There is also a risk that secrets are overproduced. Treverton's argument, that the challenge in intelligence has shifted away from information collection to analysis suggests that the information contained in 'secrets' is a less essential ingredient in informing intelligence outputs.

Part 3 combines the arguments of Professor Alasdair Roberts, Thomas Blanton, Gregory Treverton and Dr Paul Monk to demonstrate that there are cases where greater information flows are essential to enhance national security. This approach recognises that while secrets may be a by-product of the intelligence business, the purpose of security intelligence is to inform decision-makers (Treverton, 2001, 12). By incorporating the approach to information developed by Professor Peter Swire, it is possible to identify when secrecy helps and hinders security. The current approach which equates secrecy with security should be rejected. Transparency can not only help democracy and economic efficiency, but also security itself.

Part 1: The Australian Problem

> "One of the most important reasons for such non-disclosure is national security. It is hardly necessary to explain why nations must keep secret their defence arrangements." (Australia, 1978)
> - former Australian Prime Minister Malcolm Fraser

While there is 'universal acceptance' (Mendel, 2003, 4) that some secrecy may be necessary for national security, it does not follow that total secrecy is demanded. It is important to explain, and analyse the argument that nations must keep their defence arrangements secret, in order that our rights to access government held information may be pursued in tandem with our collective right of national security.

The interaction between the Australian *Freedom of Information Act* and questions of national security have received almost no critical attention in the Australian literature. The recent report of the Australian Law Reform Commission (2004) into Classified Information made eighty recommendations to the government, forty six of which were excellent suggestions on how courts and tribunals might better deal with confidential information. Recommendation 4.7 touched on freedom of information, recommending that a freedom of information request be a trigger of a document's security classification to be reviewed. The ALRC added little to its 1995 review (Australian Law Reform Commission, 2004, para 3.33).

In 1995, the Australian Law Reform Commission and the Administrative Review Council undertook a comprehensive review of the *Freedom of Information Act.* The Commission made one hundred and six recommendations for improving freedom of information in Australia, but accepted at face value the proposition that "[i]nformation about national security and defence warrants unqualified protection." (para 9.3) With regard to the exemption of Australian intelligence agencies from the act, the Review was satisfied that there was no need for those agencies to be covered by the act given that 'the vast majority of their documents would be exempt' and that the statutory and Parliamentary (i.e. Westminster) accountability mechanisms were sufficient (para 11.13). The interaction between freedom of information and national security is yet to enjoy much critical scrutiny. Even as successive waves of transparency initiatives saw the right to access government held information being enacted in the 1982 legislation, defence secrecy remained largely unaffected (Terrill, 2000, 229).

The key Australian security organisations, Australian Security Intelligence Organisation (ASIO), Australian Secret Intelligence Service (ASIS) and the Office of National Assessments (ONA) are not subject to the *Freedom of Information Act*, along with the Defence Signals Directorate (DSD) and the Defence Intelligence Organisation (DIO) (s 7(1)). Documents originating from these agencies are also

exempt (s 7(2A)). This wholesale exclusion has been followed in the United Kingdom (Wadham and Griffiths, 2003, 91), and presently by Ireland (McDonagh, 1998, 205). The blanket exclusion of security organisations has not been adopted in the United States, Canada or New Zealand (Eagles, Taggart and Liddell, 1992, 145). This is a clear 'trump card' approach, where the right of access to government held information is denied without any attempt to balance rights.

National security information is covered by section 33 of the Act. Information is withheld which "would, or could reasonably be expected to, cause damage to" (s33(1)(a)) the "security" (s33(1)(a)(i)), "defence" (s33(1)(a)(ii)) or "international relations of the Commonwealth" (s33(1)(a)(iii)). This particular formulation was adopted to match the security classification "Classified" (Australian Senate, 1979, 189), although the security classification system and the freedom of information regime were deliberately kept separate (Australian Senate, 1979, 187). The word 'damage' was especially approved because it was able to express the notion of degrees of damage (Australian Senate, 1979, 189). But considerations of degree are not evident in the way the act is implemented today. Even documents which have no security classified information are withheld on the basis of section 33 (*McKinnon v DFAT,* para.23). This approach in Australia can be contrasted with that of the United States, where the properly classified documents are exempt (The Freedom of Information Act, 5 U.S.C. § 552 (b)(1A)), which provides a much closer nexus between the freedom of information regime and the system the classifications system.

The case of *Dunn v Department of Defence* illustrates the low threshold-test for damage. The case concerned a request by a journalist for the casualty estimates concerning Australia's deployment in Operation Falconer in Iraq. The AAT reviewed a claim of section 33 exemption by the Department of Defence. The Tribunal endorsed the statement in the 1995 ALRC/ARC report that 'information about national security warrants unqualified protection' (Australian Law Reform Commission, 1995, para.118).

Although the Tribunal accepted that a "mere assertion that information is said to relate to the Commonwealth's defence or security" is insufficient to trigger the exemption (para.121), it was sufficient that the documents "could add another piece to the jigsaw or to confirm what an adversary previously only estimated" (para.128).

Once this threshold is triggered, there is no further balancing of rights. This argument is commonly referred to as the 'mosaic' or 'jigsaw' argument. It reflects the Cold War intelligence paradigm, in which scarce pieces of information were critical to solving intelligence puzzles (Treverton, 2001, 102), but the impact of the information economy has been to dramatically increase the amount of information available (Treverton, 2001, 107). Although some pieces of information may still have great security value, the value of an average piece of information in defence becomes less significant in the information age.

According to Greg Terrill's (2000, 230) review of "Secrecy and Openness" in Australia, while Australia adopted a United States' freedom of information model, it retained classic Westminster deference to the executive in matters of defence and security (Terrill, 2000, 144). This is evident in the adoption of conclusive ministerial certificates. The *Freedom of Information Act* permits a government Minister (or his delegate) (s33(5)) to assert conclusively that a document is exempt for national security reasons (s33(2)). A limited right of appeal is available to the Administrative Appeals Tribunal (AAT), but the only review power is whether the minister had 'reasonable grounds' to issue it (s58(4)). The Senate Committee which reported on the 1978 Freedom of Information Bill found that it would be inappropriate for the Tribunal to decide to release once prejudice was found to defence, security or international affairs (Australian Senate, 1979, 194).

A conclusive certificate was challenged in the case of *McKinnon v Department of Foreign Affairs and Trade* presided over by Justice Downes of the AAT. The applicant, a journalist, had applied to the department for information concerning David Hicks, an Australian detained by the United States of America in Guantanamo Bay. The request sought correspondence with the United States government concerning Hicks, as well as legal advice relating to Hicks' detention. In upholding the validity of numerous ministerial certificates claiming section 33 exemptions, Justice Downes wrote:

> There is evidence before me that release of this information could reasonably be expected to cause damage to the international relations of the Commonwealth with the United States Government. The evidence that disclosure could cause damage to Australia's international relations is rational – it is

> based on reason, or reasonable. The evidence is credible. (para 20)

Provided that the threshold question of *some* evidence is met, the system of ministerial certificates moves the decision from the legal to the political spheres. Exempted intelligence agencies, ministerial certificates, and low-threshold tests combine in Australia to deny the right to access government held information, when it concerns security or defence matters. Release is effectively a matter of executive discretion, rather than through claim of legal right.

Part 2: Applying information economics to national security.

> We want to spend our resources protecting the things that are worth protecting. (United States, 1997, 50)

If the Australian approach to national security information is to be integrated with more general rights such as the right to access government held information, it is necessary to develop a common currency through which conflicting rights may be balanced. This paper will attempt to demonstrate that a quasi-economic analysis may provide this framework. The purpose of this approach is to reject a 'trump card' approach, in order to judge the costs and benefits of secrecy. This approach has been applied previously to examine compliance with freedom of information legislation in government business enterprises (Hubbard, 2004).

The information asymmetry

Secrecy creates an artificial scarcity of information; by its definition, a secret is a piece of asymmetric information. An information asymmetry arises between parties, one of whom has access to information to which another has no access. Information asymmetries are thus a source of power (Curtin, 2003, 100). The delegation of public power to agents naturally involves information asymmetries (Stiglitz, 2004, 25). Assuming the state is run by economically (and bureaucratically) self-interested actors, information asymmetries give rise to 'rent-seeking' behaviour (Stiglitz, 2002, 35). But information asymmetry between government and citizen limits democratic participation and accountability; removing information asymmetries allows for meaningful popular participation and oversight of government (Stiglitz, 2003, 7).

From the economist's perspective, some information asymmetries are necessary, as they can encourage the collection or creation of information which would not be created in a fully transparent system (Stiglitz, 2003, 25). Some security information in particular would not be volunteered by individuals if confidentiality was not assured. This argument lead to the exemption of the Australian Security Intelligence Organisation (ASIO) from the original *Freedom of Information Act* (Australian Senate, 1979, 122). With particular relation to security functions, Treverton (2001, 147) observes that effective field operations may be stifled by bureaucratic forms of accountability. Decisions under both Australian and international freedom of information regimes have justified non-disclosure on the basis of protecting the in-flow of information (McDonagh, 1998, 211).

The other argument, within the Australian context, is that secrecy is a requirement to do business with United States intelligence agencies (Terrill, 2000, 229). However, this effect does not explain the phenomenon that old materials are available under the United States' freedom of information legislation, concerning Australia, which is unavailable under the Australian process (Ricketson, 2001, 27). Furthermore, while Australia may have little bargaining power with regard to the United States on security matters, bilateral information security arrangements with similar-sized powers, such as Canada, are harder to explain (Roberts, 2004a, 415). The argument that secrecy is the price of doing business does not fit a coherent theory of information law.

Part 3 - Costs and benefits of secrecy

> Government officials may try to enhance their power, by trying to advance specious arguments for secrecy, and then saying, in effect, to justify their otherwise inexplicable or self-serving behavior 'trust me ... if you only knew what I knew.' (Stiglitz, 2003, 26)

The rubric of secrecy shields scrutiny of the motivations of secrecy. The legitimacy of a secret cannot be fully verified without giving it away in the process (Stiglitz, 2000, 1449). One of the dangers of this situation is the potential for 'bracket-creep' of secrecy, where a core of secrets, legitimately beneficial to national security, also hide a penumbra of private interests (Aftergood, 2000). An extreme example is the

Chilean experience, where the honour of public authorities is claimed as matter of public security (Gonzalez, 2003, 185).

Formal prohibition though, does not prevent informal release. Terrill (2000, 237) has written about the informal release of information in the Australian political context. Australian security information, despite a strong official commitment to secrecy (228), is subject to leaks (217). Some leaks are made with a genuine intention to preserve the national interest (224) while others are made to advance personal political fortunes (223). Formally preventing the disclosure of information, in the national interest, gives individuals power to release information informally, for their own purposes. This form of 'partial' accountability can hardly be part of a coherent information law.

Whether through bureaucratic procedures or physical safeguards, excluding individuals from information is costly (Stiglitz, 2000, 1448). Within the Australian context, determining the cost of secrecy is difficult; Australian agencies are unable even to estimate the number of secrets they hold (Australian National Audit Office, 1999-2000). Where secrecy is regarded as synonymous with security, it is the cost of doing business.

Secrecy may also limit the effectiveness of intelligence analysis. Treverton (2001, 10) argues that in the information age, the challenge for intelligence has shifted from collection to analysis and verification of information. But even in the United States, security intelligence proceeds in the Cold War paradigm of information as a scarce resource (Treveton, 2001, 2). In Australia, important open sources can be neglected (Monk, 2002, 43). This is hardly useful when considering that the purpose of intelligence agencies is not to produce 'secrets', but to give policy makers an insight into the minds of others (Treverton, 2001, 5).

The Australian National Audit Office (1999-2000, 2.84) has found that wrongly classified information is most likely to be over-classified. The Australian Law Reform Commission (2004, 4.25-4.47) considered this issue in some depth. The policy of minimizing secrets and the undesirability of over-classification is well understood; however, there was concern expressed over the degree of training and experience of public service staff in classifying documents (Australian Law Reform Commission,

2004, 4.43). The ALRC noted that unlike New Zealand and the United States where the authority to classify rests at high levels, classification in Australia is made by the 'originator' of a document (Australian Law Reform Commission, 2004, 4.47). To counteract over-classification, the ALRC recommended administrative disciplinary action where classification standards for documents were breached, similar to the disciplinary sanctions available for contravention of the United States' executive order on Classified National Security Information (Australian Law Reform Commission, 2004, 4.46).

Unlike the United States' scheme, the security classification system is not directly connected to release under freedom of information. But a tendency to over-estimate the potential harm of document disclosure by an agency, will necessarily effect the judgment of an FOI officer within that agency to determine that release could reasonably be expected to damage security, defence or international relations (*Freedom of Information Act*, 1982, s 33).

The current system of security classification and secrecy was developed after World War Two, when information was still a scarce resource (Treverton, 2001, 102). With the development of information technology, the sheer quantity of information has become overwhelming (Treverton, 2001, 2). As the supply of information increases, the cost of each piece of information has dropped, and it never pays to have just a little (Stiglitz, 2003, 13). If information is both over-produced and over-classified, the resources required to protect these secrets is compounded.

Part 4: When openness is best.

This part looks at the potential benefits of greater transparency. The first argument for transparency is to enhance security by engaging the citizen in an analytical capacity, outside of the intelligence bureaucracy. The second argument for transparency is that security information directly empowers citizens to take action against security threats. The countervailing argument against transparency is then considered; that information will fall into the 'wrong hands'. Importantly, this argument does not undermine the arguments for transparency, rather, it asserts that the benefit of transparency is outweighed by the potential costs involved if the information is misused. However, adopting Professor Peter Swire's analysis of

'information uniqueness' provides us with a tool for determining when disclosure will help or hinder security.

The Citizen Analytical Engine

Professor Alasdair Roberts (2004b, 74) and Thomas Blanton have argued for a more transparency in national security so that citizens can contribute in an analytical role. Rather than regarding national security as an untouchable domain of government, Roberts (2004b, 69) seeks to engage the citizen. The promise of this argument is both accountability and better policy (Blanton, 2002, 9). This argument rightly rejects the notion that the right to government information and national security are mutually exclusive (Blanton, 2003, 64). This 'open approach' to security information is based on a scientific paradigm, where advancement requires that knowledge be shared (Blanton, 2003, 59). It has been adopted by the open source software movement (see http://www.opensource.org/), whose mantra, with respect to computer security, is 'no security through obscurity' (Swire, 2004).

The argument for citizen engagement requires people, outside of government, who are sufficiently well informed about security and intelligence to contribute meaningfully to public policy debate. This is not always the case. In Canada, Wesley Wark (2001) has observed that the media, with little inside understanding of security and intelligence seeks out "isolated and ephemeral stories of failure, institutional breakdown, and scandal". Wark's solution to this problem in Canada is to call for a greater out-flow of information from the Canadian Security and Intelligence sector, so that external interest and capacity can be developed. Furthermore, the insights of experts outside the security intelligence franchise, such as academics, financial analysts (Treverton, 2001, 108) or investment bankers may be equally fruitful (Monk, 2002, 52) may be able to contribute to national discussion on security.

Benefits of Openness – Direct Empowerment

Elaine Scarry's (2002) argument for security transparency is the direct empowerment of citizens. Scarry's article considered the capacity of passengers aboard Flight 93 on September 11, 2001 to prevent the hijackers on board from carrying out their mission. She argues that a group of informed citizens will be able, in some situations, to engage in more effective national defence than an institutional response. Here the actors in this case happened to be the passengers on board. The intelligence which they received was that two planes had already been flown in to

buildings that morning. This removed an information asymmetry between the hijackers and the passengers, notably that the hijackers had no intention to safely land the plane. As such, the risks which passengers were prepared to take to resist altered dramatically. While this may be more an example of self-defence, than national security, the crash-landing of the aircraft into fields, rather than another building, was clearly a positive national security outcome.

The Flight 93 scenario though is the exeption rather than the rule. As Treverton (2001, 140) argues, the output of the intelligence cycle is to give better understanding to those who must act. While direct provision of information may be decisive in some circumstances, it is unlikely that the institutional provisions in freedom of information legislation will deliver these outcomes. Nevertheless, Scarry's example is useful for showing that security sometimes mandates openness.

The Wrong Hands

Arguments for transparency in national security appear reckless (Roberts, 2004b, 69) due to the danger of information falling into the wrong hands. While transparency may produce better public policy in the long run, it is argued that security must be effectively defended today. While a transparent system may empower friendly citizens, it runs the risk of empowering enemies of the state. It is at this point that the right to government held information seems to be trumped by the duty to provide a secure state. The terror attacks on September 11, 2001 have reinforced the contention in the minds of both the public and policy-makers as to just how high the stakes are when it comes to national security (Blanton, 2002).

But using the 'wrong hands' argument to argue for blanket secrecy of security information, is just as limited as using the 'direct empowerment' argument for complete transparency. Rather, there will be pieces of information for which the 'wrong hands' argument is compelling, but many cases where it is not. If national security is to be balanced against the right to access to information, then it is necessary to develop a framework with which to answer the 'wrong hands' question. Adopting this approach, the overproduction of secrets can be minimized. Necessary secrets can be protected, otherwise the right to government held information can be respected, and the citizen can be engaged.

Information Uniqueness

Professor Peter Swire (2004) has developed a calculus for determining when secrecy will help, and when it will hinder security. Swire has adopted a quasi-economic methodology in the context of computer security. His approach is to consider when information disclosure will help 'attackers' and when it will help 'defenders'. He presents his work in a 2x2 Matrix:

		Help the attackers effect	
		Low	High
Help the defenders effect	High	Open Source	Information Sharing
	Low	Public Domain	Military

Swire's 2x2 Matrix

Within the 'military' paradigm (the classic national security example relating to the location of troops), the value to 'attackers' will be high, while the potential to help 'defenders' is low. It is within this paradigm that the 'wrong hands' argument is strongest. Making information available in this paradigm will not help national security, and is more likely to undermine it. Therefore, information asymmetry may be justified within this paradigm as public disclosure would come at great cost to national security without the prospect of great benefits.

The opposite to the 'Military' Paradigm is the 'Open Source' paradigm. It is this approach that underlies modern approaches to computer security, that there is 'no security through obscurity'. Where potential attackers to a computer network are able to share information on vulnerabilities quickly and cheaply, there is little value in maintaining secrecy. Rather, the best approach is share as much information as possible, to allow a network of 'defenders' to improve security. The 'Open Source' paradigm effectively provides the basis of the arguments discussed later in this paper, that the wider distribution of national security information can in fact contribute to security, through the 'Citizen Analytical Engine'.

The experience of Dr Paul Monk (2002, 52) within Australia's Defence Intelligence Organisation (DIO) appears to be an example where information policy operates

unnecessarily within a military paradigm, when the open source approach may yield better results. Monk was head of the DIO's China analysis, but was prevented from pursuing insightful discussions on Asian affairs with Bill Overholt, the head of Asia research for Bankers Trust. Despite the fact that the information being discussed was unclassified, Monk was required to cease contact on the basis that Overholt was not security cleared. The obsession with secrecy, perhaps required in the military paradigm, undermines the capacity of the organisation to operate within the open source paradigm.

The 'Information Sharing' paradigm relates to information which is of high value information to both attackers and defenders. Swire uses the example of terrorist watch lists at airports. To provide any benefit to security, there must be effective flow of this type of information between agencies and governments. Maintaining information asymmetries within this paradigm is essential, as the information in the 'wrong hands' undermines security.

Lastly, information within the 'Public Domain' paradigm is already well known or widely available. As such, it is of little value to either attackers or defenders. This argument was in fact accepted in *Dunn v Department of Defence*, with regard to certain pieces of information which were already available, such as the capacity of certain aircraft. The AAT found that the release of documents would not damage the security of the Commonwealth, as the information sought could be reliably gleaned through open sources.

By examining these paradigms, Swire has developed a function for determining the 'uniqueness' of information. Essentially, information which is highly 'unique' will provide security benefits if kept secret. Information which lacks the quality of uniqueness does not warrant secrecy, as the secrecy does not in fact benefit security. Within the 'open source' paradigm, secrecy will hinder security. This uniqueness is a function of the initial protective effectiveness of information, the ability to alter that defence, the number of possible attacks, the ability of an attacker to learn from previous attacks, and the organisation and communication between attackers.

Swire's analysis allows us to reject the assumption that secrecy is necessary for security. It provides a conceptual tool to determine in advance when the release of information under access legislation will in fact harm national security, and when

secrecy is of little or no value. Adopting Swire's approach to secrets provides a calculus by which we may protect only the secrets worth keeping.

Part 5: Conclusion

The relationship between national security and freedom of information in Australian has not been studied in significant depth. More so than in other jurisdictions, the rights of Australians to access government held information do not practically apply when it comes to national security. The underlying assumption is the secrecy is necessary to protect national security. The combination of excluding intelligence agencies, conclusive certificates and a low-threshold test means that at no point is the value of secrecy weighed against the rights of citizens in transparency.

The 'trump card' effect for security information in Australia is much greater than in the United States, Canada or New Zealand. The United States has a close nexus between security classification and freedom of information, and all three countries have most of their security and intelligence agencies subject to freedom of information processes. As such, the issue of secrecy against transparency is at least open to debate. However, within Australia results are largely a foregone conclusion. Like the recently enacted United Kingdom legislation, the Australian *Freedom of Information Act* combines the exemption of security agencies, ministerial certificates and low-threshold harm tests, with the result that security and intelligence matters can not be opened for debate.

The economic perspective provides an insight into why this is not a desirable state of affairs. Blanket secrecy creates information asymmetries, creates and environment for rent seeking, in the form of inefficiency, corruption or leaks. Adopting the language of micro-economics provides the common currency with which the right to access government held information can be weighed against, not trumped by, national security. Aside from the costs of secrecy, there are strong arguments that transparency can, in many cases, contribute to national security. As such, it is necessary to break down the Australian assumption that secrecy equals security. In many cases, an open network of intelligence analysis may provide better security outcomes than closed networks. By applying Swire's analysis, we are given criteria with which to judge the efficacy of security.

Apart from the removal of ministerial certificates, and the inclusion of security agencies under the *Freedom of Information Act,* these insights do not require wholesale change of the Act. Rather, the arguments presented, coupled with Swire's analysis, should be used to develop coherent criteria upon which section 33 exemptions can be examined. For the foreseeable future, deference to the executive in national security matters is likely to remain. However, by showing how transparency can help not only democracy, but also the public purse and security itself, a more coherent paradigm can be adopted by decision makers within government.

Looking beyond Australia, this paper has applied tools of information economics to the hard case of national security. By adopting this approach, it has been possible to consider the underlying questions of information flow within the 'special domain' of national security. It addresses the issues in terms of creating rational and efficient flows of information, without being spooked by the high stakes which surround national security as a political concept. The use of information economics allows us to abandon approaches which treat information differently according to their discrete legal categories. It provides a coherent and unified approach to information theory, which will hopefully be able to underpin a unified and coherent treatment of information law.

Reference List

Cases:

McKinnon v Department of Foreign Affairs and Trade [2004] AATA 1365 (21 December 2004)
Dunn v Department of Defence [2004] AATA 1040 (4 October 2004)

Statutes:

Freedom of Information Act 1982 (Cth)

Books, Journals, Articles:

Aftergood S (2000) Secrecy is back in fashion *Bulletin of the Atomic Scientists* 56:6 (http://www.thebulletin.org/article.php?art_ofn=nd00aftergood)

Australia (1978) Attorney-General's Department *Protective Security Handbook,* Canberra: Australian Government Publishing Service

Australian Law Reform Commission (1995) *Open government: a review of the federal Freedom of Information Act 1982*, Report 77

--- (2004) *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, Report 98

Australian National Audit Office (1999-2000), *Operation of the Classification System for Protecting Sensitive Information*, Report 7

Australian Senate (1979) Parliament. Senate. Standing Committee on Constitutional and Legal Affairs., Missen, A J. *Freedom of Information Bill 1978, and related aspects of Archives Bill 1978*

Blanton T (2002) The Openness Revolution: The Rise of a Global Movement for Freedom of Information *Development Dialogue* 1

--- (2003) National Security and Open Government in the United States: Beyond the Balancing Test in *National Security and Open Government: Striking the Right Balance* New York: Campbell Public Affairs Institute

Curtin D (2003) Digital Government in the European Union: Freedom of Information Trumped by Internal Security in *National Security and Open Government: Striking the Right Balance*, New York: Campbell Public Affairs Institute

Eagles I, Taggart M and Liddell G, (1992) *Freedom of Information in New Zealand*, Oxford: Oxford University Press

Gonzalez F (2003) Access to Information and National Security in Chile, in *National Security and Open Government: Striking the Right Balance* New York: Campbell Public Affairs Institute

Hubbard P (2004) Accountability in the grey area: Employing Stiglitz to tackle compliance in a world of structural pluralism, a comparative study, *FoI Review* 111:26

Mendel T (2003) National Security vs. Openness: An overview and status report on the Johannesburg principles, in *National Security and Open Government: Striking the Right Balance*, New York: Campbell Public Affairs Institute

McDonagh M (1998) *Freedom of Information Law in Ireland*, Dublin: Roundhall Sweet & Maxwell

Monk P (2002) Breaking the addiction to secrecy: intelligence for the 21st century *FoI Review* 101:42

Ricketson M (2001) Freedom of information and authors: an unsung treasure trove *FOI Review* 94:26

Roberts A (2001) Structural Pluralism and the right to information *University of Toronto Law Journal* 51:3, 243-271

--- (2004a) A partial revolution: The diplomatic ethos and transparency in intergovernmental organizations in *Public Administration Review*, 64.4 (July/August 2004): 408-422 (Lead article)

--- (2004b) National security and open government, *Georgetown Public Policy Review* 9.2 (Spring 2004): 69-85

Scarry E (2002) Citizenship in Emergency: Can democracy protect us against terrorism? *Boston Review* 27:5 (http://www.bostonreview.net/BR27.5/scarry.html)

Stiglitz J (2000) The Contributions of the Economics of Information to Twentieth Century Economics, *Quarterly Journal of Economics*, 115(4)

--- (2002) Transparency in Government, in *The Right to tell: The role of mass media in economic development*, Washington D.C.: World Bank

--- (2003) Information and the Change in the Paradigm in Economics, Part 1 *The American Economist* 47

--- (2004) Information and the Change in the Paradigm in Economics, Part 2 *The American Economist* 48

Swire P (2004) A Model for When Disclosure Helps Security: What Is Different About Computer and Network Security? *Journal on Telecommications and High Technology Law,* Vol *2* http://ssrn.com/abstract=531782

Terrill G (2000) *Secrecy and Openness: The Federal Government from Menzies to Whitlam and beyond* Melbourne: Melbourne University Press

Treverton G (2001) *Reshaping National Intelligence in an Age of Information*, Cambridge: Cambridge University Press

United States (1997) Commission on Protecting and Reducing Government Secrecy, *Secrecy,* Washington DC: US Government Printing Office

Wadham J, Griffiths J (2005) *Blackstone's Guide to The Freedom of Information Act 2000*, Oxford: Oxford University Press

Wadham J, Modi K (2003) National Security and Open Government in the United Kingdom in *National Security and Open Government: Striking the Right Balance*, New York, Campbell Public Affairs Institute

Wark WK (2001) Canadian Access to Information Review Task Force, *The Access to Information Act and the Security Intelligence Community in Canada*, Report 20