



**Open Government:  
A Journal on Freedom of Information**

[www.opengovjournal.org](http://www.opengovjournal.org)

## **Table of contents Volume 1 Issue 3**

### **Table of Contents**

- Editorial
- Paul Hubbard: Freedom of Information and Security Intelligence: An economic analysis in an Australian context
- Sarah Holsen: First pulse check on UK FOI community indicates good health
- Timothy Pitt-Payne: The role of the information tribunal under the UK Freedom of Information Act 2000
- Heather Brooke: The UK's openness watchdog lacks teeth and transparency
- Book review: Heather Brooke: Your right to know
- Book review: Patrick Birkinshaw: "Government and Information The Law relating to Access, Disclosure and their Regulation"

## Editorial

Steve Wood

Editor

Open Government: a journal on Freedom of Information

[s.wood@livjm.ac.uk](mailto:s.wood@livjm.ac.uk)

**Volume 1 issue 3 December 2005**

### Welcome

Welcome the 3<sup>rd</sup> issue of "Open Government: a journal on Freedom of Information", the end of the first year of the journal's life. The journal now has an extensive worldwide readership that we intend to build on in 2006. Thank you all the authors and reviewers who have worked with the journal during 2005. The aim for 2006 is to expand readership and attract more detailed research based articles whilst still seeking high quality viewpoint articles and brief communications.

Next year the journal will feature articles on the following topics:

- Freedom of Information in the EU
- Freedom of Information in Germany
- Freedom of Information and confidentiality
- Freedom of Information and Privacy Law interaction
- Freedom of Information in New Zealand
- Freedom of Information and the development agenda in Africa

I welcome articles from around world on the topic of Freedom of Information legislation. I'm also interested to hear from readers with views about issues of themes that the journal needs to cover.

As the journal is open access and non-commercial we have a limited budget for promotion, so please do pass on and promote the journal if you deem it be to be relevant to others. If you are willing to distribute a poster or some flyers at events, conferences etc please contact me at the email address below.

**This issue's articles**

This issue contains an interesting discussion by Paul Hubbard from University of Tasmania about national security information in the context of Australia using theories from information economics to challenge assumptions of secrecy. This issue also contains three articles from the UK, which this approaching the end of its first full year of implementation: Sarah Holsen from University College London outlines the results of a practitioner survey, UK Barrister Timothy Pitt-Payne discusses the Tribunal System under the Freedom of Information Act 2000 and finally Heather Brooke outlines her perspective on the performance of the UK Information Commissioner during 2005.

Best wishes for 2006 to all readers

Steve Wood

Editor, [s.wood@livjm.ac.uk](mailto:s.wood@livjm.ac.uk)

**Author:** Paul Hubbard, University of Tasmania

Private Bag 89 Hobart Tasmania 7001

[phubbard@utas.edu.au](mailto:p Hubbard@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 led 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 (Treverton, 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 exception 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 an 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](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 21<sup>st</sup> 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 Telecommunications 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



**Author:** Sarah Holsen, UCL Constitution Unit

**Title:** First pulse check on UK FOI community indicates good health

**Volume 1 issue 3**

Central government departments and local authorities in the UK recorded a total of approximately 47,000 Freedom of Information Act requests between 1 January and 30 June 2005<sup>1</sup>. Although the number of requests decreased over the six-month period, the total volume reflects a significant amount of work carried out by public officials and civil servants to comply with the Freedom of Information (FOI) Act in the first half of the year. How did they cope? In order to 'take the pulse' of the FOI community, on 16 June the Constitution Unit distributed a survey to FOI practitioners attending the *Third Annual Information Conference for the Public Sector: FOI Live 2005*<sup>2</sup>. The survey results suggest that practitioners found the process of implementation a smooth one, albeit with a few challenges, and that they believe they did well in responding to requests in the first half of the year.

133 delegates from central and local government, the NHS, universities, and other organisations subject to the FOI Act completed the questionnaire<sup>3</sup>. Of those who responded, 32 per cent (43) worked for central government departments, 18 per cent (25) for a public body or quango, 17 per cent (22) for local authorities, 11 per cent (15) for NHS departments and 5 per cent (6) for universities. 61 per cent of respondents reported that they were the primary FOI practitioners for their organisation and all but 9 per cent of respondents had responsibilities other than FOI compliance, most in the areas of data protection, records management and/or the Environmental Information Regulations.

<sup>1</sup> This figure was reached by adding the total number of requests to central government reported in the Department for Constitutional Affairs' *Statistics on Implementation in Central Government Q1: January – March 2005* (23 June 2005) and Q2: *April – June 2005* (30 September 2005) (<http://www.foi.gov.uk/statsapr-jun05.htm>), as well as the estimated total number of requests to local authorities reported in the Constitution Unit's *Freedom of Information: The first six months – The experience of local authorities in England* (30 September 2005) please contact the Constitution Unit for more information – [s.holsen@ucl.ac.uk](mailto:s.holsen@ucl.ac.uk)".

<sup>2</sup> The conference was jointly organised by the Constitution Unit, Department for Constitutional Affairs and the Information Commissioner's Office and attracted delegates from both the public and private sectors. The focus of the conference was assessing the first six months of freedom of information compliance in the UK and identifying areas that need attention.

<sup>3</sup> The total number of conference delegates was 347. Because no sampling techniques were used, we cannot claim that the data are statistically significant. A copy of the survey questions can be obtained by contacting Sarah Holsen, Research Fellow at the Constitution Unit, at [s.holsen@ucl.ac.uk](mailto:s.holsen@ucl.ac.uk).

Overall, practitioners felt their organisations were prepared for FOI and that they effectively met the challenge of responding to requests. Over 75 per cent of respondents reported that they were satisfied with the level of training received prior to implementation, whilst only 11 per cent believed that the key FOI staff in their organisation had *not* been adequately trained. Practitioners also reported that they found the volume of requests manageable - almost half (41 per cent) of all respondents received between one and 100 requests over the first six months, whilst local government practitioners received between 101 and 300, and five practitioners reported receiving more than 1000 requests (two of whom were from central government departments). The ability of public organisations to effectively handle implementation of the Act was also reflected in the fact that the majority of FOI practitioners (84 per cent) claimed to have met the statutory 20-working day response deadline 'most of the time' (only 4 per cent admitted to meeting the deadline less than half the time). However, there was concern about the adequacy of resources their organisations had dedicated to FOI compliance, e.g. staff or software. Just over half (52 per cent) believed that their organisation had sufficient resources to handle the requests they received.

The survey also suggests that if the Act's success were based on rate of disclosure, it succeeded in the first half of the year. Most practitioners reported that their organisations disclosed the information requested; indeed, more than half of respondents stated that their organisations did not refuse or only partially refused to disclose information for more than 80 per cent of requests they received. However, the survey also found that 16 per cent did refuse to disclose information and did so for over half of all requests they received. This figure increased to 22 per cent when taking into account only central government respondents.

The types of information requested suggest that people are using the FOIA to demand greater openness and accountability from public institutions. Respondents reported that the category of information most frequently requested was information related to the management or use of public funds (56 per cent), followed closely by information relating to government policies/plans at 50 per cent. Information concerning government contracts, licensing /regulatory decisions and other business transactions formed a substantial proportion of the remainder of request types.

Who was making the requests? Because the Act is requester blind, i.e. requesters do not have to disclose the capacity in which they're making a request, an exact answer is impossible. However, when asked to guess the top three categories of requesters, practitioners stated that they believed most were private individuals (reported by 118 practitioners) and journalists (reported by 100). Coming in a distant third, fourth and fifth were business employees/executives, academics and students, and NGOs/pressure groups. Although the FOI practitioners suggested private individuals were the most frequent requesters, it is possible that requests from business people (especially small business), for example, could appear to have come from private individuals. Nevertheless, if one puts the data together, most information requests seem to come from private individuals who are concerned with the management or use of public funds and with particular aspects of government policies or plans.

Despite the fact that most practitioners reported few significant problems with implementation, they did face some challenges. The top three problems mentioned by practitioners (in order) were applying the public interest test (28 per cent), coordinating with sections of their organisations that held the requested information (28 per cent) and figuring out whether their organisations held the information requested (22 per cent). When asked which topics they'd like addressed in the form of guidance, respondents listed balancing the public interest test, handling repeated and vexatious requests, and dealing with requests for personal information. Most practitioners (54 per cent) reported turning to colleagues when faced with a problematic FOI request, followed by the Department for Constitutional Affairs (35 per cent) and senior management (31 per cent). It is clear from the survey results that formal and informal networks of support were considered valuable sources of advice and support - over half reported subscribing to a support/advice network. The most frequently mentioned FOI practitioner network was the JISC Mail email discussion list (<http://www.jiscmail.ac.uk/lists/FREEDOM-OF-INFORMATION.html>), though only 11% of the surveyed practitioners stated that they subscribe.

In summary, practitioners' responses to the survey give the impression that the FOI community as a whole was adequately trained, had sufficient resources and was able to deal with the volume of requests received in a timely manner during the first six months of 2005. Survey results also suggest that the implementation of the FOI Act was not as problematic as some might have expected; indeed, for many the concerns prior to 1 January seemed to turn out to be 'much ado about nothing'. There is also

evidence that there was a general acceptance of the new Act among public authorities – 51 per cent of practitioners reported that the attitude toward FOI in their organisation was positive. In short, if doctors were assessing the health of the FOI community on the basis of the Constitution Unit's brief check of its pulse on the 16 June 2005, they might conclude that it was stable and without serious ailments. However, this is only a small (and informally derived) part of the picture – larger scale sector-specific surveys of practitioners and FOI requesters should be conducted on a regular basis in order to gauge the 'success' of FOI and any changes in the level of that success and make necessary modifications to procedure and administration.

*Sarah Holsen is the research fellow on access to information and data protection at the Constitution Unit, part of the Department of Political Science/School of Public Policy at University College London.*

**Author:** Timothy Pitt-Payne

Barrister, 11 King's Bench Walk Chambers, UK

**Title:** The role of the information tribunal under the UK Freedom of Information Act 2000

**Volume 1 issue 3**

If freedom of information (FOI) legislation is to be of any real value then it must include a means of resolving disputes and enforcing compliance. The relevant provisions of the UK's Freedom of Information Act 2000 (FOIA)<sup>4</sup> comprise two main elements. First, a dissatisfied applicant for information may apply to the Information Commissioner for a decision under FOIA section 50 as to whether his request has been dealt with in accordance with the Act; secondly, either the complainant or the public authority may appeal to the Information Tribunal ("the Tribunal") against the Commissioner's decision. There is a further right of appeal from the Tribunal to the High Court on a point of law<sup>5</sup>. This Note considers the role of the Tribunal under FOIA.

The Tribunal is not a newly created body. In its previous incarnation as the Data Protection Tribunal it considered appeals under the Data Protection Act 1998 ("DPA 1998"),<sup>6</sup> and it retains this jurisdiction. FOIA has given the Tribunal a new name, and has greatly increased its importance and likely workload.

The Tribunal consists of a legally qualified chairman and deputy chairmen, together with non-lawyer members. There are two categories of member sitting in FOIA cases: those appointed to represent the interests of applicants for information, and those appointed to represent the interests of public authorities. For most purposes the Tribunal will consist of the chairman or a deputy chairman (presiding), together with two members, one from each category. This "interest representation" model is familiar from the workings of the Employment Tribunal system, where lay members

---

<sup>4</sup> The Freedom of Information (Scotland) Act 2002 has a different regime, not discussed in this Note.

<sup>5</sup> The Tribunal also considers appeals against information notices or enforcement notices issued by the Commissioner, under FOIA section 51 or 52.

<sup>6</sup> And prior to that, under the Data Protection Act 1984.

are appointed to represent either employer or employee interests and the chairman is a lawyer<sup>7</sup>.

The relevant rules of procedure are contained in the Information Tribunal (Enforcement Appeals) Rules 2005 ("the 2005 Rules"). There is not space for a detailed analysis, but a few points of particular interest are noted below.

Under rule 16 the Tribunal has a discretion as to whether to determine cases at a hearing or on paper; the Tribunal must however hold a hearing if a party so requests, unless satisfied that the case can properly be determined without a hearing. It is suggested that relevant factors in deciding whether to hold a hearing may include: whether the case raises issues of general importance; whether there are difficult issues of law, on which oral argument would assist; and whether there are conflicts of fact which might be resolved by cross-examination of witnesses. So far a number of cases have been listed for oral hearing, but this may partly reflect a desire by the Tribunal to use the early cases in order to give general guidance on the operation of FOIA; hence the Tribunal's willingness to list cases for oral hearing may decrease with time, once a significant number of cases has been decided.

The appellant will be either the individual who complained to the Information Commissioner or the public authority that was the subject of the complaint. The respondent will in every case be the Information Commissioner. Thus the Commissioner has an unusual role under the Act: under section 50 he exercises a quasi-judicial function, but in appeals to the Tribunal he is a party, defending his own decisions. There are good pragmatic reasons for this. In appeals brought by public authorities it would clearly be unsatisfactory if the individual complainant, very likely without legal representation, was left with the task of defending the Commissioner's decision in his favour.

Where the appellant is the individual complainant, then the public authority will not automatically be a party to the appeal – and *vice versa*. However, the individual complainant or public authority may be joined as additional parties, on their own application or by the Tribunal of its own motion, under rule 7 of the 2005 Rules. Other parties may also wish to be joined. For instance, where a commercial

---

<sup>7</sup> The special rules about the constitution and jurisdiction of the Information Tribunal in national security appeals are not discussed in this Note.

organisation has supplied information to a public authority, and the issue is whether that information should be disclosed in response to a request under FOIA, the commercial organisation may well apply to be joined under rule 7.

The Tribunal's powers in determining appeals against decision notices are defined in FOIA section 58<sup>8</sup>. The Tribunal must allow the appeal or substitute another decision notice if the decision notice is not in accordance with the law, or if any relevant discretion of the Commissioner ought to have been differently exercised. Otherwise, the appeal must be dismissed. The Tribunal may review any finding of fact on which the Commissioner's decision was based. Some interesting questions will need to be resolved about the scope of these powers, especially in cases involving the application of the qualified exemptions under FOIA. In applying these exemptions decision-makers must balance the competing public interests in disclosing the information in question and in upholding the exemption. It remains to be seen whether the Tribunal will simply substitute its own view for that of the public authority or the Commissioner as to where the balance should be struck, or whether it will adopt a more cautious approach.

An obvious practical point is this: can the Tribunal itself see the information that is in dispute? Clearly if the Tribunal is to do this then the individual who is seeking the information cannot be permitted to see it too – this is the very question at issue in the appeal. Under the 2005 Rules the Tribunal has a limited power to exclude one of the parties from the hearing (see rule 23: the power is exercisable only on application by a Minister of the Crown), but no specific power itself to examine information without disclosing that information to a party. Contrast DPA 1998, under which a Court considering a dispute about the right of subject access conferred by section 7 of that Act may examine the disputed information without disclosing it to the data subject: see DPA 1998 section 15(2).

At the time of writing<sup>9</sup> the Tribunal's website lists 15 appeals currently being processed. Usefully, the website also gives the time and location of forthcoming hearings. There are three FOI decisions on the website: *Mitchell v Information Commissioner*, *Barber v Information Commissioner*, and *Harper v Information Commissioner*. Detailed analysis of these decisions must await a further article.

---

<sup>8</sup> The same provision applies to appeals against information notices or enforcement notices.

<sup>9</sup> 6<sup>th</sup> December 2005.

Within the next three to six months there is likely to be a significant volume of Tribunal case law, with the potential to be of great value to all those who need to interpret and apply FOIA.

## References

Data Protection Act 1998. Chapter 29. HMSO. Available online at:  
<http://www.opsi.gov.uk/acts/acts1998/19980029.htm>

Freedom of Information Act 2000 Chapter 36. HMSO. Available online at:  
<http://www.opsi.gov.uk/acts/acts2000/20000036.htm>

The Information Tribunal (Enforcement Appeals) Rules 2005. SI 2005 no. 1. HMSO.  
Available online at: <http://www.opsi.gov.uk/si/si2005/20050014.htm>

Information Tribunal Website: <http://www.informationtribunal.gov.uk/>

**Author:** Heather Brooke, freelance journalist ([www.yrtk.org](http://www.yrtk.org))

**Title:** The UK's openness watchdog lacks teeth and transparency

**Volume 3 issue 1**

## **The UK's openness watchdog lacks teeth and transparency By Heather Brooke**

- ***Information Commissioner fails to meet his own deadline***
- ***Default position is secrecy***

The UK watchdog charged with ensuring that public bodies obey the new Freedom of Information Act already has a huge backlog of appeals that will take years to clear. An even greater surprise is that these figures, along with early decisions, were withheld and were only made public after filing an FOI request.

The Freedom of Information Act 2000 and Freedom of Information (Scotland) Act 2002 both came into force 1 January 2005. The two countries' laws are similar but each country has its own Information Commissioner. In the UK, just over 22,000 FOI requests have been received between 1 January and 30 June 2005 by the 42 central government bodies monitored by the Department for Constitutional Affairs<sup>10</sup>. The Scottish Executive reported that from 1 January to 5 April it received approximately 900 requests for information that were centrally recorded by the Executive's Freedom of Information unit.

Applicants must first exhaust a public authority's internal review process before appealing to the Commissioner, even though in 79 per cent of cases, public authorities uphold their initial refusal. The table below shows the statistics for the UK and Scottish Information Commissioners as of 4 November 2005<sup>11</sup>.

	UK Commissioner	Percentage of total received	Scottish Commissioner	Percentage of total received
Closed cases	640	31%	99	21%
Decision notices	69	3 %	44	9%
Ongoing	1325	65%	327	70%
Total number of applications	2034		470	

Even at the quickest rate of issuing decisions - 16 in July, it will take the UK Commissioner more than eight years to clear the present backlog.

<sup>10</sup> Freedom of Information statistics for Q1(1 Jan-30March) and Q2 (1 April-30 June 2005)

<sup>11</sup> Figures from James Ford, spokesman for the UK Information Commissioner's Office and Claire Sigsworth, spokeswoman for the Scottish Information Commissioner.

Whereas the Scottish Commissioner, Kevin Dunion, has committed to dealing with cases within four months, the UK commissioner has been reluctant to state any similar performance targets. However, at the Society of Editors conference in Cumbria 17 Oct 2005, Deputy Commissioner Graham Smith stated the Information Commissioner's Office (ICO) has now set a minimum target of resolving 50 percent of cases within 12 working weeks. But caseload data is not published on a regular basis, so there is no way of knowing if this most basic target is being met.

The Commissioner had four years to prepare for implementation of the FOIA. In addition, the ICO paid for a study published March 2004 (Hazell, 2004) by University College London's Constitution Unit, which predicted the number of appeals and subsequent staff needed. The study forecast that between 1250 and 3000 appeals would be received during the first year – an entirely accurate prediction.

Not every request can be predicted, of course, but the most contentious were certainly well known. The Attorney General's advice to Tony Blair on the Iraq War had been sought since March 2003, yet when the appeal came to Commissioner Richard Thomas, he was unable to commit to a date for delivering his verdict. In the end the information was leaked to the media. Restaurant inspections, fire safety inspections, and the names of MPs' staff were all predicted as being major FOI test cases, and yet to date, the commissioner has failed to make a decision on appeals seeking exactly this type of data.

### **Early decisions and case lists kept hidden**

The UK Commissioner even seemed unprepared to issue decisions. The Scottish Information Commissioner published his first decision 17 May 2005. I telephoned the UK Commissioner's press office to see if any decisions had been issued. A spokeswoman told me there were 10 decisions to date but they were unavailable. After two weeks, they were still not public, so I made an FOI request for the decision notices 1 June.

I received the first 11 decisions by email on 15 June and posted them on the 'Your Right to Know' website [www.yrtk.org](http://www.yrtk.org). The next day, Mr Thomas told an audience at the FOI Live 2005 Conference in London<sup>12</sup>, that there had been a policy of secrecy. "Perhaps we were a little nervous before in not publishing," he told the conference delegates, "but we are changing our policy and I'm announcing today that summaries of all our decisions will be published online 48 hours after they are made."

As well as publishing decisions, the Scottish Commissioner also publishes a list of all the cases his office has under investigation on a monthly basis.

"Publishing the decisions? It's not something I ever thought of *not* doing," Dunion said (interview 11 August 2005). "And I thought it would be useful to put up our database of cases under investigation because it helps people to see what kind of information others are asking for and hopefully that encourages the public to use the Act."

The UK Commissioner does not publish such a list, and so on 1 June 2005 I filed an FOI request for this information. The answer came back on the last day of the

---

<sup>12</sup> FOI Live 2005: Third Annual Information Conference for the Public Sector held 16 June 2005 at Victoria Park Plaza, London

statutory time period (30 June), yet the number of cases on the database was just 368 when the Commissioner stated his office had received over 1,000 appeals. Where were the remaining 600+ cases?

After a month of chasing, the final database came through on 4 August 2005, long after the statutory time period had elapsed. The delay arose, I was told, because the ICO had misunderstood my request for "a listing of all complaints received and their file numbers" to mean only a partial listing.

To date, the only place to view the caseload database is on my website<sup>13</sup>, and unfortunately the data I was given excludes detail on what the request was for but it does give case numbers and the name of the public authority in question.

The accuracy of the data is questionable. For example, the database includes two entries for Norfolk County Council, yet Norfolk's corporate FOI Officer, Deirdre Sharp, contacted me to say the council has had no communication from the Commissioner about either of these requests, one of which the council has no knowledge. A citizen, Denis McCready, contacted me 21 October 2005 to say his organisation has filed three applications with the ICO about refusals to see extracts from the 1911 and 1921 censuses for England & Wales and the 1937 census for Northern Ireland<sup>14</sup>. He says: "Although the ICO has acknowledged our complaints, the case database doesn't list two of our complaints and our case against the Office for National Statistics shows that our case was closed months ago. That's news to us!"

Publishing a list of the cases under investigation is the only way for the public and even public authorities to accurately assess who is using the act and the Commissioner's effectiveness. ICO is still refusing to publish this data. "I realise you would like the caseload to be made public on an ongoing basis," said ICO spokesman James Ford. "Compiling that information takes time – time and resource we currently spend on dealing with appeals."

### **Weak Decisions**

Of the Commissioner's 64 published decisions, only three have ordered disclosure. In the vast majority of cases, the Commissioner had taken so long to make a ruling that the public authority had already 'answered' the request, even if that meant issuing a proper refusal notice. The Commissioner was unable to take any punitive action, even in the cases where public authorities flouted the law either by failing to respond in time, ignoring the request or denying the request without legal reason.

The three orders for disclosure are against local authorities rather than central government. Bridgnorth District Council, Shropshire, (Case Ref: FS50062329) was ordered to release council files in a land dispute. Corby Borough Council (Case Ref: FS50062124) was told to release salary details of a temporarily employed finance officer. Luton Borough Council (Case Ref: FS50064062) was ordered to release correspondence related to a land sale.

In other cases, ranging from a list of the revenue generated by speed cameras to information about how council tax bands are calculated, the Information

---

<sup>13</sup> <http://www.yrtk.org/secret-squirrel/ic-caseload/>

<sup>14</sup> McCready has posted a summation of his cases at: <http://home.clara.net/denis.mccready/index.htm>

Commissioner sided with the public authority, or simply declared that a refusal notice had not been properly issued.

Where a complainant's account differs with that of a public authority, the Commissioner has given the benefit of the doubt to the public authority. For instance, he accepted that the Human Fertilisation & Embryology Authority "complied with the Act in posting a response to the complainant within 20 days", even though the complainant stated no such letter had ever been received.

Matthew Davis, news director of John Connor Press Association, will become one of the first people to take his appeal to the Information Tribunal after the UK Commissioner upheld the National Maritime Museum's refusal to disclose to Davis the cost of a public sculpture (Case Ref: FS50063478). He is still waiting for a decision about his complaint filed with the ICO on 7 February against Sussex Police's refusal to release the number of registered sex offenders.

"I suspect they (the Commissioner's Office) are worried sick about giving out information that has never been disclosed before," Davis said (interview, 29 September 2005) "So they just stall and stall, hoping it will leak out like the Iraq War advice."

Davis is also dubious about the Commissioner's handling of requests: "One of the first cases I sent to the Commissioner's Office was lost," he said. "I only discovered it when I received an acknowledgment letter for another complaint. When I called up they said it had been lost and that I'd need to re-send the file, so I did - this time by registered post."

Both public authorities and applicants have cited the ICO's severe lack of communication as a problem. Some authorities such as Norfolk are not aware they are even under investigation, whereas applicants (including myself) are left in the dark for many months. Written guidelines (section 19, Memorandum of Understanding) state that the ICO should communicate with applicants every 28 days, yet this is not happening.

Stephen Gradwick, a consultant in Merseyside who has made almost 40 FOIA requests said (interview 26 September 2005) the only way he has been able to keep track of his cases was by telephoning the Commissioner's Office. "They are just not being helpful or user-friendly, and I'm given no information about the status of my cases unless I ring. At one point, the Deputy Commissioner Phil Boyd then sent me an email telling me to stop enquiring about my cases."

It is admirable that Richard Thomas has spoken out against government secrecy, but this must be followed with tough action. The first step would be to institute greater transparency in his own office, making it an example for other public authorities to follow.

## Bibliography

Brooke, H. (2005) *Your Right to Know*. Pluto Press

Department for Constitutional Affairs: Freedom of Information Statistics (online)

Q1: <http://www.dca.gov.uk/foi/statsjan-mar05.htm>

Q2: <http://www.dca.gov.uk/foi/statsapr-jun05.htm>

Hazell, Robert; Baxter, Dick; Cook, Meredith; Maer, Lucinda (March 2004) Report: Estimating the likely volumes, sensitivity and complexity of casework for the Information Commissioner under the Freedom of Information Act 2000 and the Environmental Information Regulations. University College London: Constitution Unit and available online at:

<http://www.informationcommissioner.gov.uk/cms/DocumentUploads/Final%20Document.pdf>

Information Commissioner's Office (March 2005) Memorandum of Understanding (MoU) between the Secretary of State for Constitutional Affairs (on behalf of government Departments) and the Information Commissioner, on co-operation between government Departments and the Information Commissioner in relation to sections 50 and 51 of the Freedom of Information Act 2000 (the "FOI Act") (including ss.50 and 51 as applied, as amended, by Regulation 18 of the Environmental Information Regulations 2004).

Information Commissioner's Office: Listing of Decision Notices (online)

<http://www.informationcommissioner.gov.uk/eventual.aspx?id=8617>

Scottish Information Commissioner's Office: Monthly listing of validated cases (online)

<http://www.itspublicknowledge.info/appealsdecisions/investigations/index.htm>

Scottish Information Commissioner's Office: Decisions issued by the Commissioner (online) published within a week of the decision being issued.

<http://www.itspublicknowledge.info/appealsdecisions/decisions/index.htm>

**Book review**

Heather Brooke (2004) *Your right to know: how to use the Freedom of Information Act and other access laws*. London. Pluto. ISBN 0745322727.

**Volume 1 issue 3**

**Review** by Susan Healy, National Archives

Heather Brooke has produced a bravura account of access rights, and the dire effects on the public good if they are ignored. It is written with great sincerity but not quite as great accuracy.

The stated aim of the book is 'to give you the tools to get the information you want. It tells you what your rights are and how to use them' (page 1). By 'you' she means members of the public, and the focus is very much on helping them find information of use to them. There is also frequent encouragement to readers to exercise their access rights, either by suggesting topics that could be pursued or by recommendations such as 'if you are a Londoner and only send one FOIA request in your lifetime, there is no more deserving recipient than Transport for London (page 92).

The book has many strengths. One is its scope: she does not confine herself to FOI but sets out to cover a wide range of access rights to particular types of information. These are dealt with in separate chapters: central government; intelligence, security and defence; transport; the justice system; law enforcement and civil defence; health; the environment; local government; education; private companies; and information about individuals. As well as outlining access rights for each category she suggests useful starting points for obtaining information. These include details of key bodies, with a description of the type of information they hold and the address to which enquiries should be sent, and references to websites and printed sources that can be used to identify and locate many others. From this point of view the book will be invaluable to those seeking information but not knowing where to start.

Another strength is her inclusion of comparisons with rights of access overseas, especially in the USA. The many examples she gives of openness in other countries will enable those seeking information in the UK to argue 'if they can why can't you' – although whether that will be persuasive remains to be seen.

The layout is clear, with boxed in summaries of key facts and an index at the end. There are also model request and appeal letters.

However, there are some deficiencies that suggest she has not fully understood some of the legislation she describes. For example, the chapter 'Information about individuals' deals with both subject access rights and rights of access to personal information about third parties but never mentions the key fact that the Data Protection Act applies only to information about living individuals. She has completely misunderstood the concept of 'historical records' (page 18) – records become historical records by virtue of their age not their access status. She confuses the exclusion of some bodies from the FOI Act altogether and the exemption of information from or about them held by bodies subject to the Act (the security and intelligence agencies at pages 73-75 and the courts at page 99).

She is very shaky on the difference between Parliament and Cabinet (page 34) and on the position of MPs (also page 34), for example 'As a Member of Parliament the Prime Minister is subject to the Freedom of Information Act and to make a request you can either contact the PM's office directly or preferably send your query to the Cabinet Office'. She is only partly correct in her description of which private bodies might be subject to the Environmental Information Regulations, omitting the important criterion that the private body must be under the control of a public body (page 179-180). These just a few examples and the frequency of errors do, in the opinion of this reviewer, undermine the usefulness of the book.

In summary, this is a rattling good read but should be used with caution because of the errors it contains.

**Book review**

Patrick Birkinshaw (2005) Government and Information The Law relating to Access, Disclosure and their Regulation. London. Tottel Publishing. ISBN 1845920880.

**Volume 1 issue 3**

**Review** by Ibrahim Hasan, ActNow Training.

Patrick Birkinshaw is an experienced and widely published public lawyer. This is the third edition of this book which has been revised to take account of the plethora of legislative developments in this area particularly the coming into force, on 1<sup>st</sup> January 2005, of the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

The first chapter is devoted to a thorough discussion of Freedom of Information Act 2000, particularly the application of the exemptions drawing upon the Information Commissioner's guidance notes. Some discussion of the latest decisions of the Information Commissioner would have been useful. However I suspect the book was completed a few months ago when there were not many meaningful decisions to comment upon.

A comparison is also made between the 2000 Act, the various Freedom of Information Bills and the Government's previous White Paper on this subject. This allows the reader to understand how far the ideals of openness and transparency have been sacrificed at the altar of political reality. There is also mention of the differences between the Scottish and the English Freedom of Information Acts. Only seventy six pages out of a total of six hundred and sixty are devoted the Freedom of Information Act. This is perhaps not surprising bearing in mind the title of this book. Those seeking more detail can look at other books and also guidance published by the Information Commissioner Office (ICO) and the Department fro Constitutional Affairs (DCA).

The beauty of this book is in its discussion of many different applicable statutes and legal cases, which together make "information law", and their application to different parts of the public sector. For example, in the central government arena one has to consider the Official Secrets Act 1989, the Public Interest Disclosure Act 1998 and the D Notice system.

For those in local government, the discussion of specific functions such as council tax, economic development and the information law provisions specific to them will be interesting to those grappling with the interaction of such legislation with Freedom of Information. The Local Government Act 1972 (as amended) is examined in the context of the new executive arrangements and the conduct of meetings. There is a good table comparing the latter with the Freedom of Information Act as well as one setting out all the statutory provisions which require local authorities to publish information

A whole chapter is devoted to access to personal information and privacy. The author examines the Durant decision and its impact on the definition of personal data. Legislation covering the health sector is also discussed e.g. the Access to Medical Records Act 1988 and the Access to Health Records Act 1990. Data matching and information sharing are also given some space. Although a lot of this refers to the ICO guidance and the DCA toolkit there is a useful examination of the European perspective. Those in the police sector may wish to read the section on data held by the police and also the implications of Bichard Inquiry. There is also useful mention of the ACPO guidance on weeding old records as well as the guidelines on the use of the Police National Computer.

Information Law is a rapidly expanding area of law. This kind of book greatly contributes to its understanding and debate. It will suit lawyers, academics as well as those who are seeking to learn about the bigger picture not just Freedom of Information. At around £70 it is also very good value.

**Ibrahim Hasan was formerly a principal solicitor at Calderdale Council (UK). He is now a writer and trainer on information law issues with Act Now Training Email: [ibrahim@actnow.org.uk](mailto:ibrahim@actnow.org.uk)**

---

