Breaking the addiction to secrecy: intelligence for the 21st century

One of the most persistent problems in contemporary Western democracies is the over-classification by governments of the thinking processes behind controversial policy decisions. Whether in Australia, the United States or Britain, virtual Chinese walls are in place to shield governments against accountability, in both foreign and domestic affairs. Freedom of information is an official piety, not a public reality. This has damaging effects on decision making itself and on democratic norms. Yet governments seem addicted to secrecy and deeply averse to transparency. This has to change.

Nowhere is the addiction to secrecy more serious than in the area of strategic intelligence. It is as if the polar opposite of economic wisdom about protectionism and free trade is dominant. Information is so relentlessly protected that its circulation and the quality of its production are badly impeded. Cutting down the 'tariff barriers', however, threatens many interests, makes many government officials feel insecure and all too easily generates paranoia about the imagined monsters and enemies who lurk on the other side of those barriers. Yet they must come down.

The case for keeping secrecy to a minimum is not new. Like free trade theory, it has been around for some considerable time. It was Lord Acton — famous for his remark that 'All power corrupts and absolute power corrupts absolutely' — who declared in the 19th century, 'Everything secret degenerates, even the administration of justice; nothing is safe that does not show how it can bear discussion and publicity'. Yet, like the argument for free trade, it has to be made again and again, against entrenched opposition.

The Cold War triggered a huge increase in the size and extent of the Chinese walls of secrecy in the West — to say nothing of the totalitarian states. When it ended, the Clinton administration flirted with the idea of substantially dismantling them. On 30 April 1994, under Public Law 103-236, it created the Commission on Protecting and Reducing Government Secrecy. On 3 May 1997 the Commission issued its report. Its opening sentence was: 'It is time for a new way of thinking about secrecy'.

We should create a new era of openness to replace 'the culture of secrecy ... that we associate with Dulles and Hoover', it recommended. Not just because the danger had passed, but because secrecy had added to the danger at the height of the Cold War and inhibited insights which might have brought it to an end sooner.[1] In fact, decades before the Commission did its work, a series of US government commissions with the highest credentials had urged that secrecy be drastically curtailed. Yet none of them had any substantial effect. The quantity and range of documents being classified continued to grow. The Pentagon classified literally billions of pages of material, losing all perspective on the rationale for or consequences of such classification.

One of the most interesting cases of fruitless recommendations for openness is that of the Defence Science Board's Special Task Force on Secrecy in 1970, which argued that secrecy ran directly counter to the nature of the scientific research whose technological work it sought to conceal. It argued that, all things considered, the US would be better off if it adopted, *unilaterally if necessary, a policy of complete openness in all areas of information.* This task force was not composed of naïve or fellow-travelling 'liberals'. It included such notable cold warriors and weapons scientists as Edward Teller and Jack Ruina of MIT. But their report was disregarded — and classified 'For Official Use Only'.

Undeterred by 50 years of specialist 'Canute' commissions trying to stem the tide of secrecy, Gregory Treverton has once more attempted to make the case for cutting down secrecy and developing a culture of openness.[2] He is a senior consultant at RAND, with many years experience in intelligence and strategic policy affairs in Washington. He argues that two flaws in traditional intelligence work — excessive secrecy and the disconnect between the worlds of intelligence analysis and policy making — must be overcome in the 21st century. They can only be overcome, he believes, by systematic overhauling of the way both analysis and policy-making are done. And openness will be the key to the paradigm shift.

With the extraordinary super-abundance of information and the rapidity of the changes in its configurations in the world we now live in, the practices of secrecy, compartmentalisation and the separation of intelligence from policy have become hindrances to clear and critical thinking, Treverton writes. He seems unaware that this has long been so, but he is clear that it is more true than ever and that, in consequence, a fundamental reshaping of intelligence institutions is called for. Above all, intelligence officers need to be directly in touch with the best thinkers in the world outside their organisations. They need to seek out both experts with information they lack and information brokers who can assist them in complex processes of analysis.

'Conceiving of intelligence as information, not just secrets, would begin to provide arguments for new priorities and for reshaped institutions', Treverton writes. 'Sadly, intelligence has been moving in exactly the opposite direction. For instance, the intelligence community created the Community Open Source Program Office (COSPO) as a focal point for innovation in using open sources, but by the late 1990s COSPO was ... wound down, as intelligence returned to a preoccupation with secrets.'[3]

This is the old addiction kicking in. Its effect is to cut intelligence analysts off from much that is going on. 'At the NIC (National Intelligence Council)', Treverton remarks drily, 'we used to quip that if academics sometimes did better than intelligence analysts, it was because [they] weren't denied access to open sources!' Trapped inside their world of secret channels and classified compartments, intelligence officers too easily succumb to the illusion that, if something doesn't come through those channels, 'it doesn't exist' and if it's not in their compartment then it's not their responsibility. 'For instance, CIA analysts can do competent assessments of particular industrial sectors in given foreign countries. Yet, alas, they usually do so in ignorance of what Wall Street or other private sector analysts are doing, sometimes better.'[4]

A classic case history which shows the need for the changes Treverton calls for is that of the intelligence failures before the Mexican peso crisis in 1994. His story corroborates Paul Krugman's analysis a year *before* the crisis.[5] 'As the storm clouds gathered around Mexico's finances during 1994', Treverton relates, 'intelligence had begun paying more attention', but for the most part its warnings were 'never very sharply etched and so were dismissed by Treasury', where the prevailing view was that Mexico could and would ride out the pressure it was under, without undergoing a currency devaluation.

An exception was the National Intelligence Council's senior officer for warnings, who monitored open source information about the rapid depletion of Mexico's foreign exchange reserves in its efforts to prop up the peso and talked to the minority of Wall Street analysts who were bearish on Mexico. She warned, in early 1994, that Mexico would be forced to devalue the peso. As Treverton emphasises, '[her] strength was that she reached out to (the Wall Street sceptics); she broke out of the isolation that was — and is — all too characteristic of American intelligence.'[6] The 'ostensible experts mostly dismissed her', but she was right.

As it happens, 'neither [her] arguments nor those of her critics depended on secrets. The information was there. The art lay in interpreting and projecting it ... Mind-sets mattered more than secrets.'[7] This is where Treverton might have driven home his underlying point more powerfully than he did. For the truth is, mind-sets *always* matter more than secrets. Mind-sets are the filters through which secrets, like any other information, must pass *en route* to the making of a policy decision. Yet they remain for the most part invisible or unexamined.

The practice of secrecy helps keep the mind-sets of intelligence analysts and policy makers invisible. It is not the only thing which does so, of course. For human beings, of their nature, are prone to cognitive biases and blindspots which vitiate their thinking whether or not they are shut up in a world of secrets and classification. The point is that that sort of confinement — and the conceits which go with it — tends to increase the likelihood of such things going undetected and uncorrected. Secrecy in regard to information turns policy makers into modern day alchemists or astrologers: practitioners of a secret art based on esoteric knowledge. It was Francis Bacon who wrote 400 years ago of such esoteric pseudo- sciences that they were 'full of error and vanity' which were veiled and concealed 'to save the credit of impostures'.[8]

The quest for sound policy must go via the search for a rigorous testing of assumptions and mind-sets, rather than a search for and a tenacious keeping of secrets. As Treverton remarks, 'Often lines of analysis or of policy are based on half-buried assumptions. To counter this tendency, intelligence would need to interrogate policy about its assumptions or mind-sets, then try to validate or discredit the assumptions'.[9] This rarely happens, because policy makers seldom encourage it and often actively discourage it. Moreover, lines of inquiry which would be useful in challenging such assumptions and mind-sets conducted outside the classified world are often entirely overlooked.

The first thing to change is the perception that 'intelligence' consists of 'products' — classified pieces of paper or firewalled data on computer screens. Such things, as Treverton points out, 'are only inputs. The output of intelligence is better understandings in the heads of people who must decide or act.'[10] It follows from this that the nature of understanding itself must be a primary focus of the intelligence craft.

It follows, further, that the policy makers, even more than the intelligence analysts, need to develop the skills of making their assumptions explicit and opening them up for critical examination. The *corrigibility* (the openness to testing and correction) of beliefs and mind-sets then becomes the cardinal virtue of intelligence analysis and policy making practice. Seeking the means to make this possible is epistemic leadership — leadership committed to the integrity of thinking.

Incorrigibility is the cardinal sin of both intelligence and policy practitioners. It is the stock in trade of sycophants who gather around ruthless leaders, reinforcing their vanity and their misplaced confidence in their own judgement. This does any leader a disservice, because unwillingness to learn, not lack of vital secrets, is the greatest source of strategic error. Such unwillingness often leads to suppression of information which would expose errors of judgement.

For decades now, standard intelligence training manuals have described what is called the intelligence cycle. It consists of four stages: direction, collection, analysis and dissemination. The policy makers give direction as to what they want to know about. It is collected by spies, satellites and electronic surveillance. It is analysed in the light of policy concerns and then disseminated to those needing to act.

Treverton argues that things are messier and more complex than this. This is true enough. The real key to the matter, though, is that *the fifth stage in the intelligence cycle is always omitted.* In between dissemination and (new) direction the cycle should show *learning.* But it never does. This is a remarkable indication of the virtually universal blindness to the haphazard and costly ways in which learning takes place in intelligence and policy organisations — where it takes place at all. Clearly, it is taken as given that intelligence *in some way* modifies understanding and therefore makes strategic adjustment possible. But just *how* understanding is modified is not in the picture. Secrecy serves to ensure that it never will be. Yet learning is the absolutely crucial stage in the cycle.

The argument against the culture of secrecy is, therefore, a severely practical one. Past a certain very minimal point, secrecy impedes the development of understanding, inhibits learning and leads to enormous waste of resources, in the form of useless or unused intelligence 'products'. The argument for openness is that it is necessary in a world of complexity, in which there is a superfluity, not a scarcity of information; and necessary just in so far as one wants effective, corrigible and responsible policy making.

Treverton suggests five steps be taken, by way of crossing the doctrinal Rubicon and breaking the addiction to secrecy. First, position the intelligence analysis centres as close as possible physically to the policy- making centres. Second, open the intelligence agencies to real experts, giving integration of analysis priority over cumbersome security requirements. Third, reshape intelligence agencies to lead the open source revolution, instead of leaving them on their secret islands to become cognitive dodos. Fourth, ensure that intelligence analysts are dispatched out into places where serious thinking takes place, rather than being corralled in 'secure' cloisters. Fifth, conduct substantial experiments in how best to

make policy assumptions or mind-sets explicit and corrigible.

These are excellent and, of course, radical suggestions. Treverton, though, is a pragmatic individual. 'Any effort at serious reform', he acknowledges, 'must search for points of leverage'.[11] And such points can be obstinately defended. Just how much resistance there is to even the simplest and most practical of steps he discovered when the CIA required that he delete from his book a story about an *unclassified* NIC project, which he wanted to publish in order to get some public recognition of good intelligence work. He had told himself, when he first joined the NIC, that 'I should stay only as long as I could continue to laugh at the peculiarities of the CIA culture, such as classifying my schedule'. The censorship of his 'unclassified' NIC project made him stop laughing.

Not long before I left the world of secret intelligence myself, I had an experience rather more telling than Treverton's. I was head of China analysis at the Defence Intelligence Organisation (DIO) and had, at my own initiative, developed an excellent rapport with Bill Overholt, then head of Asia research for Bankers' Trust, Hong Kong. Dialogue with him about Asian affairs was more enlightening than the great bulk of classified information that came across my desk. Just as the dialogue was getting places, however, my DIO division head told me that I must cease my communications with him, because he was 'not security cleared'.

That I was not sending Bill any classified information seemed to be irrelevant. That he had one of the finest iconoclastic minds in the Asia analysis world meant nothing to my benighted bureaucratic boss. When I pointed out that Bill had better access all around the Pacific rim, from Beijing and Tokyo to Washington, than anyone in the DIO, the division head merely repeated, like a mantra, that he was not security cleared. The instruction stood. Like Treverton, I stopped laughing and, not long afterwards, left the DIO. It is not enough to laugh at the pathologies of the secret world. We need to reform it.

PAUL MONK

Paul Monk is a principal with Austhink, a Melbourne-based research, training and consulting group.

Austhink assists organisations and individuals to think more effectively. It specialises in critical thinking, with particular focus on argument mapping, the use of software-supported graphical techniques to enhance the mind's capacity to process complex reasoning on any issue. Dr Monk's essays appear frequently in the Friday ReView supplement of the *Australian Financial Review* and in *Quadrant*. A web site of his writings can be found at <http://www.austhink.org/monk/>.

This article first appeared in the Australian Financial Review, 1 March 2002.

References

1. Moynihan, Daniel Patrick, *Secrecy: The American Experience*, Yale University Press, 1998. For an extended discussion of this book, which is based on the Commission's work, see Monk, Paul, '*Arcana Imperii:* Secrecy and Responsible Government', (1999) January/February *Quadrant* 33-43.
2. Treverton, Gregory F., *Reshaping National Intelligence For An Age of Information*, Cambridge University Press, 2001.
3. Treverton, above, ref 2, p.113.
4. Treverton, above, ref 2, p.108.
5. Krugman, Paul, 'Challenging Conventional Wisdom', a speech delivered in Mexico City in March 1993, subsequently published as Chapter 9 in his delightful book *Pop Internationalism*, MIT Press, 1996.
6. Treverton, above, ref 2, p.95.
7. Treverton, above, ref 2, p.97.
8. Bacon, Francis, *The Advancement of Learning*, quoted by Gaukroge, Stephen, *Francis Bacon and the Transformation of Early Modern Philosophy*, Cambridge University Press, 2001, p.7.
9. Treverton, above, ref 2, p.208.
10. Treverton, above, ref 2, p.107.
11. Treverton, above, ref 2, p.249.

Access and Privacy in Canada

Developments from September 2001 to August 2002

Introduction

This article summarises the main developments that have taken place in access to information and privacy of personal information in all Canadian jurisdictions during the period from September 2001 to August 2002.

In Canada, there are two federal (Canadian) oversight regimes — one for access and one for privacy. There are also oversight regimes within each of the country's ten provinces and three territories. Broadly speaking, the two federal regimes have access and privacy responsibilities with regard to federal government departments and public bodies. Access to and privacy of the information held by other institutions, including local governments, is generally administered through the provincial or territorial regimes.

The exception is the power granted to the federal Privacy Commissioner, who, since the passage of the *Protection of Personal Information and Electronic Documents Act (PIPEDA)*, has oversight over cross-border and interprovincial exchange of personal information, as well as personal information held by federally-regulated businesses. As of 2004, this oversight will extend to all businesses in the private sector, except where provinces have their own legislation in place to cover privacy in this sector.

As a result, many provinces have recently passed or are starting to introduce their own private sector privacy laws. These laws have begun to interact with the access laws in each of the provinces, and have in some cases prompted provinces to pass access legislation where there was none before. While certain jurisdictional issues have yet to be tested, particularly with regard to the territories, a clear trend towards privacy is starting to be a factor in access circles across the country.

Legislative developments

Public sector

In June 2002, the 20-year review of the federal *Access to Information Act* took place. It was conducted by a special Access to Information Review Task Force, composed of appointed senior government officials and a body of outside advisers, rather than by a Standing Committee of the Parliament. After 18 months of evaluation, the Task Force released a report concluding that the Act itself is basically