



4th
International Conference of
Information Commissioners
MANCHESTER 2006

Conference Speech

Author: Air Vice-Marshal Andrew Vallance
Secretary of the United Kingdom's Defence Press
and Broadcasting Advisory Committee
www.dnotice.org.uk

Title: secrecy vs security; the jigsaw effect

Volume 2 issue 2

It's a great pleasure to address this very important conference. I speak to you today as the Secretary of the United Kingdom's Defence Press and Broadcasting Advisory Committee, an independent body which provides guidelines to the UK media on the disclosure of national security information.

I've been asked to speak to you on the subject of 'Secrecy vs Security', an intriguing title. The use of the term 'versus' - suggesting that 'secrecy' and 'security' are somehow inevitably in opposition - reminded me of a famous book called 'Animal Farm'. Written in the mid-1940s by George Orwell, perhaps the greatest British political literary satirist of the 20th Century, 'Animal Farm' is a biting parody of state over-control, using Stalinist Russia as its implicit model. As those of you who have read it will recall, the book begins with a rebellion by the animals of Manor Farm who feel they are being oppressed by the owner – Mr Jones. The rebellion against Jones is led by the pigs, the cleverest of the Farm's animals, who rename their community 'Animal Farm'. They announce that 'all animals are equal' and coin the slogan 'four legs good, two legs bad'. But after its high-minded beginning, Animal Farm follows a seemingly inevitable course towards inversion and reversion, with the pigs progressively controlling the other animals in the same way as Farmer Jones. In the end, the pigs move into Jones' farmhouse, learn to walk on two legs, alter the Animal Farm doctrine to 'All animals are equal, but some are more equal than others' and change the Farm's slogan from 'four legs good, two legs bad' to 'four legs good, two legs better'.

I'm won't test your patience today by trying to argue 'security good, secrecy bad', and certainly not 'security good; secrecy better'. The world is far too complex for such simplistic,

black/white, right/wrong judgements, even if I did believe that security and secrecy were necessarily alternatives: which I do not. But what I would like to offer you today is why I believe that security and secrecy can be both complementary and opposing concepts, depending on how they are implemented. The message I offer is 'security good; secrecy also good' at least at certain very specific times, in certain clearly defined circumstances, and provided that how and when secrecy is imposed, it is done so with common sense and moderation and tempered with proper instruments of oversight and public accountability.

Contemporary British society has a dialectic view of secrecy. The British people see personal secrecy – privacy it is generally called - as an inalienable right, part of the nation's birthright a fundamental component of their freedom. The introduction of measures seen to erode it are attacked widely and with full force as a matter of the highest principle, with the default setting always protecting personal privacy – except in cases of the most dire and immediate national emergencies. Pressure groups - such as Liberty - exist specifically to champion that cause and do so with great energy and determination and much popular support. 'Privacy' is indeed the word in general use here rather than secrecy, but the two in this context mean the same: the right to hold back from the public domain information about an individual that he or she wishes to remain a personal secret. In Britain, the right to personal secrecy is safeguarded in law - inter alia - by the Data Protection Act of 1998 and Article 8 of the Human Rights Act also of 1998. Journalistic secrecy is similarly seen as being critical to personal freedom through its role in ensuring that government is accountable. Journalists, and on occasion editors, or even (on at least one famous occasion) a CEO, are willing to risk public censure, even prison, to preserve their secrets, and most notably the identity of their sources.

But in the context of public governance, secrecy has an almost entirely negative popular resonance within Britain. Indeed, it is often presented as posing threats that extend well beyond the obvious areas of personal or collective freedoms, to prosperity, continued employment and individual ways of life. One could sum up the British view of secrecy as 'Private secrecy good, but public secrecy bad'.

Part of this comes from our cultural legacy: the apparently innate British preference for individual freedom and our historic suspicion of centralised government, wherever it might be based. But this preference has been mightily strengthened by the knowledge-centric society in which we now live. Information management techniques play an already dominant and still swiftly growing part in all our lives. While privacy is carefully safeguarded, official secrecy can often seem incompatible with this. For example, one of the key enabling policies of any system which seeks to impose secrecy – be it personal, commercial, military or governmental - is that of 'need to know': this aims to restrict the type and quantity of information released

to individuals to that which they really need. The theory behind 'need to know' is that it reduces the danger of, and limits the damage sustained through, security breaches, compromise or betrayal. But there are growing problems with 'need to know'. Even if one agrees with the principle, which many do not (at least when it is applied at the collective level), 'need to know' involves making highly subjective judgements. No one really knows what they (or anyone else) really need to know, until – that is - they need to know it. Indeed, deciding what people need to know is one of the most fundamental challenges facing knowledge management development. It is also a very convincing reason why people should be at liberty to search the full extent of the knowledge spectrum, as and when the need arises, to find out the particular information they need. And secrecy can only hinder that search.

But of even greater concern to the majority is the potential to exploit secrecy to abuse power. There is no question that a general culture of excessive secrecy holds serious threats to us all. Knowledge is power – today far more than ever before. And the denial of information, however obscure, is seen by some as reducing their power, while the hoarding of it by others is seen as increasing theirs. Secrecy in whatever form denies access to information which some believe to be public property by right. Secrecy applied selectively can lead people into making flawed judgements because they do not have all the pertinent facts. Applied in blanket form, it raises concerns that whole areas of government activity are being shielded from proper public scrutiny and accountability. In both forms, secrecy can erode trust in authority, appear to set one group in society above and beyond the others and raise concerns that individuals in Government, or even whole Government departments, may be out of proper control and unaccountable.

Setting aside these objections of principle, there are also some very practical difficulties in keeping secrets secret. Firstly, there is cost. Secrecy is a very expensive business, and the wider the range of secrets that have to be kept, the more difficult they become to manage, administer and police. Secrecy imposes widespread and diverse burdens on the administrative machinery which add time and cost to government processes without adding any apparent value to the products. So much so in fact that whichever preferences a government may have, its ability to impose secrecy will be limited by the capacity of its administrative machine to manage the associated procedures, absorb the constraints and still work at an acceptable level of efficiency.

Allied to that, and of rapidly increasing importance, there is the World Wide Web. The internet has become an information gathering and dissemination tool of unprecedented capacity and - outside of China at least - available to all in a pretty well unfettered form. The already

awesome power of the internet is fed only in part by the already colossal and still rapidly growing capacity and power of the international media, now more closely integrated (at least at the technical level) than ever before. A story reported in an obscure journal in a remote region can be picked up and within hours be repeated all over the World. It then remains on the Google and Yahoo data bases where it can be accessed for evermore. Once there, the use to which it can be put cannot be restricted. The terrorists who carried out the London bombings of 7 July last year – for example - appear to have gathered the information they needed to make their bombs from the World Wide Web without external assistance.

The challenges posed by the World Wide Web to those who seek to keep information secret apply not only to individual pieces of information (which can now be posted by anyone for example on web-logs or 'blogs'), but also to what can be learned through a process of aggregation. The traditional modus operandi of intelligence officers is to gather seemingly innocuous information, assemble it into a coherent mosaic and then make sensible judgements from the picture that emerges. This can now be performed to a surprisingly high level of competence by anyone with the time, wit and inclination who has access to an internet computer. Sometimes called 'the jigsaw effect', this phenomenon can lead civil or military bureaucrats down the path of even greater and more unproductive secrecy in an attempt to spot information which could form some part of a future sensitive jigsaw.

Of course, like a real jigsaw, one assembled with pieces from the internet does not always produce a true picture. Sometimes, the person assembling the jigsaw forces the individual pieces together to make the picture he believes to be the right one, whether or not it truly matches that on the outside of the box. Sometimes he feels that pieces are missing, when instead they are all there but have been wrongly assembled. Nevertheless, critics of official secrecy do have a point when they argue that the 'Web' now ensures that no secret is inviolable and thus efforts made by Governments to preserve official secrecy are ultimately likely to prove futile. But equally, governments can point out that there is no obligation on them to assemble - or even make a gift of key pieces - of jigsaw puzzles which might then be used to inflict death and injury on the people they are charged to protect. Whatever one's views are on this, I don't think that anyone doubts that the 'jigsaw effect' is a powerful factor; the dispute is centred on whether its effects are more 'good' than 'bad'.

Another practical constraint on official secrecy is the public's willingness to accept it. This is not so much 'whether or not?', but 'how much the market will bear?' In Britain, the answer to that question is 'not very much'. Moreover, attempts to extend official secrecy tend to strengthen the determination of those who claim to champion liberty and who seek to expose 'the truth' as they see it, regardless of the consequences. Little or no general opprobrium now

seems to be attached in Britain to the selective leaking of secret government papers; not a Sunday goes by without the publication of extracts from some leaked official document or other. Even when the 'leaker' is found (which is not often, given the nature of information distribution systems and the ability to take copies even with a mobile phone) he or she is often portrayed as a hero: someone who has taken a stand on principle against those who are seeking to deny to the public information which is rightly theirs. It is somewhat paradoxical that as freedom of information has expanded, conspiracy theorists have become ever more prominent. Perhaps we should not be surprised by this for secrecy arouses people's fascination, and attempts to shape the news – 'spin' – are widely resented. Official denials are now taken almost automatically by those who love 'cloak and dagger' stories as confirmation that what is being denied is in fact true; one often hears the slogan 'never believe anything until it is officially denied!'

The 'whistleblower' mentality holds that it is morally indefensible to keep information from the general public which in any way concerns them. Such a view fails on two counts. Firstly, it ignores the misuse to which certain types of information can be put by individuals or groups willing to use violence to achieve their aims. And secondly, the leaker rarely - if ever - has all the pieces in the jigsaw puzzle and, thus, lacks the 'full picture'; he/she cannot judge the range of the consequences which might flow from the information released. For example, publishing details of the timing, scope and location of imminent military or intelligence operations can warn the enemy, allow them to prepare and lead directly to loss of friendly lives, not only for those actually involved in the operation, but also – as a direct consequence - the lives of those who the operation was designed to protect. Another example is the measures put in place to protect people (both military and civilian) against – say - terrorist bomb attacks. If the terrorist knows exactly how an installation is protected, he can invariably find a way around the defences.

But perhaps I can best illustrate the need for a measure of secrecy by examining the Secret Services – arguably the most sensitive institutions of any nation. In Britain there are three Secret Services: the Security Service (more often called MI5 - which deals with domestic security), the Secret Intelligence Service or SIS (of James Bond fame and more often called MI6 - which deals with overseas human intelligence gathering) and the Government Communications Headquarters or GCHQ, which intercepts communications. All three of these Services are established by the law of the land, are publicly accountable (if not directly then certainly to the public's representatives) and are subject to careful parliamentary and judicial oversight.

These Services operate in a world of enduring fascination to the public, but they depend on secrecy to do their job of protecting the British people and the people of allied and friendly nations against a wide range of current threats. These threats include – inter alia – terrorism in all its many forms, illegal narcotics, mass people trafficking, organised crime and the proliferation of weapons of mass destruction, in addition to the more traditional counter-espionage role. The details and even the very existence of their operations - future, present and even past - and the identities of those who work for them, have to be protected by very high secrecy levels.

The possible consequences of such secrets being compromised were shown around the turn of the year when a Greek newspaper published what it claimed to be the name and photograph of the British SIS Head of Station in Athens. This was followed two weeks later by the Russian state broadcasting service showing footage of what it claimed to be four British SIS officers in Moscow accessing supposedly secret information from a transmitter receiver device disguised as a rock. These were not isolated incidents. Indeed, a cottage industry has developed in recent years – no doubt partly at least as a reaction to Secret Service secrecy - to publish the identities of Secret Service agents for the whole world to see. Such ‘secret agent spotting’ is generally looked on as some form of harmless game that embarrasses the bureaucrats and shows how clever the agent spotters are.

But it is not a harmless game. The Secret Services have to maintain a strict ‘neither confirm nor deny’ policy whether or not the person so named is one of their people. Even if that were not so the ‘never believe anything until it’s officially denied’ philosophy means that an official denial would probably be pointless. Persons named as Secret Service officers or agents are often totally separate from the Secret Services, but they and their families suffer just as badly. Whether true or false, public naming damages a Secret Services’ reputation for being able to keep its own secrets; it undermines the Services’ confidence, weakens its morale, and through that erodes personnel retention and recruitment. The collection of secret intelligence from sensitively placed human sources depends crucially on maintaining their confidence. This relationship is always very delicate and can be damaged when identities are disclosed. Naming – whether true or false - deters potential informants from contact with officers for fear of exposure. Officers whose names have been widely reported cannot subsequently be deployed across the full range of the services’ work, and thus years of training and experience needed to reach the required level of competency can quickly be ruined. And the more a name is repeated across the media, the greater the damage. The net result of such disclosures is to deny Britain valuable intelligence about hostile intent or capabilities. It is an undeniable fact that attempts to breach Secret Service secrecy harm the people directly involved (whether or not they are Secret Service members) and ultimately they can - and

often do - harm us all: that includes you and me. They ruin lives and for some lead to injury or death. For the Secret Services, secrecy is not some outdated fetish; it is the key enabler in the job they do; quite simply they cannot protect us without it.

We can draw three important deductions from all these points. Firstly, that a degree of secrecy – qualified certainly by time, subject matter, detail and oversight - is indispensable in preserving security. Secondly, that there are practical limits to how much information, and for how long, any government can keep secret. And thirdly, keeping secrets in the modern World depends on consensus and shared responsibility. The release of a highly classified secret may not damage security if it can be found only on an obscure website or journal which few if any read; de facto it remains buried. The problem for security begins when it becomes widely available in the public domain and difficult to ignore even for the most casual browser. When that happens there is no telling who might find it or to what use it might be put. And in deciding whether a piece of information is or is not widely available in the public domain, it is the media that plays the decisive role. It is ultimately they who will judge whether or not, and how widely, information is published or broadcast, and in reaching that decision they face balancing their own rights and interests against their wider societal duties and obligations.

This is the key premise that underpins the UK's Defence Advisory (DA) Notice system. Unique to Great Britain, this system emerged at the end of the Cold War from the long established 'D Notice' system, which was widely seen as a form of government censorship. The present DA Notice system was shaped to meet the very different conditions already emerging in the early 1990s, and was from the outset based on consensus and shared responsibility between government and the national media for the disclosure of national security information. The system is overseen by the Defence Press and Broadcasting Advisory Committee or DPBAC – an independent body with a joint membership of 5 very senior civil servants and 13 leading members of the UK media. All government departments concerned with national security are represented, and the DPBAC media members represent virtually all areas of the UK media. These include the BBC, ITV, ITN, Sky TV, the Periodical Publishers Association, the Newspaper Publishers Association, the Newspaper Society, the Press Association and the Scottish Daily Newspaper Society. The (book) Publishers Association have so far chosen not to be represented on the Committee, but their members nevertheless use the DA-Notice system. Links have also been established with the UK Internet Service Providers Association.

The code endorsed by the DPBAC is set down in five standing DA Notices which define the areas that the Committee considers to be at the core of national security. And that is their limit; they do not extend to any other sensitive areas which a government might wish to keep secret, such as internal policy disputes, waste, vice, scandal, corruption, failures in military

discipline and the like. They are not orders, but purely requests, ones which are framed broadly to allow scope for sensible interpretation.

I will not describe them in depth, but to give you an idea of their scope I would like to show you the various areas covered by each DA Notice. As you will appreciate, the release of details in any of these areas could allow an enemy to devise effective counters that would lead directly and quickly to the death and injury of British troops and perhaps to operational failure.

DA Notice No 2 deals with certain types of nuclear and non-nuclear defence equipment, whereas DA Notice No 3 covers highly classified codes and ciphers, related data protection measures and communication facilities, or those of NATO or other allies. Clearly, compromised codes and ciphers put at risk the classified information which they are created to protect, threatening security and indirectly lives. DA Notice No 4 deals with sensitive installations and the home details of individuals likely to be targeted by terrorists. The final DA Notice, No 5, covers the intelligence and security services, the Special Forces, and those who are likely targets for attack by terrorists.

Please note that these DA Notices have been agreed by representatives of the UK government and UK media, are published in full and can be accessed by the public on the DPBAC's website: www.dnotice.org.uk. They are framed to permit sensible interpretation and negotiation between journalists, authors and editors on the one hand, and the DPBAC Secretary on the other. They act as a societal agreement between the UK government and media to share responsibility for the disclosure of national security information, one which upholds the media's right to report in the public interest but recognises it has an obligation to ensure that the public is not damaged as a result.

The two key supporting pillars of this very British arrangement are confidentiality and consent. Journalist and editors must have confidence that when they seek DA Notice advice it will not be used against them or their story passed to competitors. Without that assurance they would cease to seek advice and the system would collapse. It was this reality, and the feeling that the Committee must retain its independent status, that led the DPBAC to conclude (apparently paradoxically) that they should not seek to become subject to the UK Freedom of Information Act 2000 or the Freedom of Information Act Scotland (2002). The Committee ensures full transparency about its policy and the debates that lead to its formulation – inter alia - by the publication in full of the minutes of its meetings on its website. But the continuing effectiveness of the system relies on individual casework, and the advice offered

by the Committee's Secretariat to government officials and to members of the media and public remaining strictly private.

The second of the system's supporting pillars is that advice offered under the system does not have to be accepted. It is a purely voluntary code, unsupported by any form of legal sanction. A journalist who seeks DA Notice advice on his/her story, is perfectly at liberty not to accept that advice, either in whole or in part. Even if advised against it, he or she is fully entitled to publish or broadcast the information concerned if, for example, he/she believes that the case made for not publishing is weak, or if a very important principle is at stake. In effect the system is meant to act as a safety net for journalists and editors; something which does not gag them but helps to ensure that they do not inadvertently damage national security.

As you will already have guessed there are many problems with this system. The voluntary nature of the DA Notice system exposes it as much to criticism from hard-liners who would prefer more draconian sanctions for perceived security breaches, as to civil libertarians who see in it a disguised form of censorship and a way of seducing the free press. It is also a very tricky system to manage. The issues involved are rarely clear cut, and usually highly subjective. They include many things about which reasonable people could disagree. Also, the media agencies who take a responsible position and seek DA Notice advice often feel disadvantaged in comparison with those who don't and who publish or broadcast damaging information regardless of the consequences. In perhaps the World's most fiercely competitive business, one in which the British media see themselves as leading players, this is very important. Associated with this, the DA Notice system is British-only, whereas news and information services and threats to security are already overwhelmingly international in their character. It also relies on consultation in an era of real-time and world-wide TV news broadcasts that can instantly put information widely into the public domain that cuts right across the code.

All of these areas of challenge can only increase in the future. As the electronic media becomes ever more technically integrated, as search engines become ever faster, more discriminating and more powerful, as people are able to access World-wide news through a growing number of gadgets and as media competition becomes ever more fierce, it will become increasingly difficult to argue that after its release that a piece of information is not automatically widely available in the public domain and easily accessed.

Does all of this suggest that the British DA Notice system, already imperfect, is likely to decline in effectiveness in the future? Perhaps so; we shall have to wait and see. But even if it does decline, would that be a good enough reason for abandoning a system which continues

to contribute to our security? What are the alternatives to it? Seeking greater secrecy through more stringent and intrusive legislation? I know of no one who wants that; and anyway, for all the reasons mentioned earlier, Britain already has what most people see as the maximum practical level of secrecy in the existing conditions. The only other alternative to that would be a free-for-all in which British journalists, denied the benefits of authoritative advice, would run the risk of inadvertently publishing or broadcasting information that would cause the death or injury of British troops or civilians. I know of no British journalist who wishes to be responsible for that either.

Someone once said that democracy is the worst form of government, with the exception of all the others. It might also be said that the DA Notice system is the worst way of providing national security media support, except for the alternatives. Secrecy like security is never absolute; it is always limited and relative. The DA system accepts that reality and works within it. In any case, Secrecy is just one of many elements in any security structure, and it has to be kept in balance with the others; in terms of national security this includes most notably public and media consent. Despite its limitations, the DA Notice system continues to be relevant and make an important contribution. It has delivered a great deal in the protection of our national security simply because it accepts that media-government relations in this area at least must be based on a partnership rather than being automatically adversarial.

At a time when a depressingly wide spectrum of groups regard the serialised mass slaughter of innocent individuals as a perfectly acceptable policy instrument, difficult balances have to be struck. One of those balances is that between security (in its widest interpretation) and secrecy. The most precious of all human rights is the right to life, and to preserve that today some information has to be kept secret. To ensure that that secrecy is not exploited for purposes other than preserving national security, it is far better that sensible people enter into a dialogue within defined boundaries as to what should or should not be placed, or at least widely repeated, in the public domain. This avoids wholesale recourse to the law courts, or – even worse - more restrictive laws formally extending the bounds of official secrecy. Such a dialogue fosters collective responsibility for something of key importance to us all, and it upholds the absolute right of the media to breach the established guidelines without the threat of legal sanction if they judge at any time that the arrangement is being exploited or that a crucial principle is being risked.

I would like to finish with two true stories about the Duke of Wellington – the man who defeated Napoleon at the Battle of Waterloo. The first was in Wellington's early days as a British commander in India. He was asked by a local ruler to disclose a particular piece of intelligence in exchange for a large bribe, a common enough transaction in those imperfect

times. The Duke looked furtively over his shoulder and, coming closer, asked if the ruler could keep a secret. The ruler's eyes lit up as he answered 'Yes, of course I can'. The Duke, with that cold aloofness for which he was to become so famous, replied in turn: 'Well, so can I!' Wellington could indeed keep secrets and did so throughout his life. When asked by Lord Uxbridge (his second-in-command and the commander of his cavalry) immediately before the battle of Waterloo what his plans were, Wellington simply replied 'To beat the French'. He followed this with an aside that 'If I thought my hair knew what my brain was thinking I would shave it off immediately'. In today's World we don't need to go to those lengths, but we should surely recognise that a degree of secrecy is indispensable for security. In trying to strike the right balance between 'secrecy and security' we can safely set aside George Orwell's Animal Farm slogan of '4 legs good, 2 legs bad', as we can also its successor '4 legs good, 2 legs better'. Instead we should recognise that - as in nature - '4 legs good, 2 legs also good' does apply here, at least at certain times, in certain carefully defined and broadly endorsed areas and provided it is applied with common sense and moderation and tempered with proper instruments of oversight and public accountability.