# STATE SECRECY OR TRANSPARENCY

# BALANCED SECRECY IN THE NEW INFORMATION AGE

**DAVID BICKFORD CB**

**19 January 1999**

State secrecy, like state sovereignty, is about to undergo radical change.

This change is being shaped by the instantaneous communication, trading and access to information now taking place across the international community. A new information age.

During the World Wars state secrecy as a whole was deemed so vital that it was guarded, even in the democracies, by the sacrifice of rights, including the lives of individuals both allies and enemies. The height of the Cold War saw little change save that the democracies introduced some elements of balance into the guarding process. Late in the Cold War, one of those elements, the European Court of Human Rights, set the standards to determine the balance between the needs of state secrecy and the rights of the individual to be informed. These standards were set in a series of land mark cases including Leander v Sweden, Hewitt and Harman v UK, K v France, and Ludi v Switzerland. In essence, those standards acknowledged that states were entitled to secrecy to protect their national security and economic well being but that the secrecy and action enforcing it must be proportionate to the state's need for protection.

The new information age is about internationalisation. Individuals with access to an on line computer can freely exchange information across the globe. Commerce is now conducted freely amongst the whole international community, limited only by state legislation and regulation. That legislation and regulation is often unable to be effective because of the international nature of the transactions conducted. For instance the OECD predicts that commercial transactions on the Internet will increase 200 times by the year 2000 to reach $40 billion per annum. There are no effective international regulations on such trade, nor is there any effective capability to assess and collect taxes on the revenues of such trade.

Internet communication is increasing ever faster. The communications, commercial or private, can be encrypted. And states have not yet agreed how to ensure decryption of those communications internationally without expending the assets of state agencies such as NSA and GCHQ to do so.

Underlying this proliferation of information lies the thrust of international competition.

The advantages of Internet commerce are being exploited as much as the advantages of information exchange. Companies trading in countries previously little known now have access to instant in depth information from public web sites. More detailed or personal information is now available via personal web sites or e mail. Former government servants, including law enforcement and intelligence officers, offer their services to gain and provide information about their own and other countries and business there. Private individuals do likewise. The financial rewards are commensurate and add to the competitive thrust to increase the availability and detail of such information.

This explosion of information exchange and availability is already piercing the secrecy safeguards of states. Because states are unable effectively to regulate or control the explosion it will continue to pierce that secrecy with deepening and broadening effect. Moreover, the costs of protecting secrecy from this increasing reach into it are prohibitive.

The explosion goes to the heart of the sovereignty of states. And, as states perceive their sovereign control weakening, they will be tempted to test the limits of proportionate response to protect their secrets.

At the same time as this phenomenon develops another has become apparent. In the past, threats to states were readily identifiable both physically and geographically. Now, the threats to states are fluid, transient, international and obscure. Terrorism comes not only in the identifiable shape of state terrorism but also in the dim images of iconoclastic groups, anarchic gangs, and eco-warriors. Terrorism now spills over to narcotics traffickers, extortionists and information warfare computer hackers. Organised crime, operating in chameleon form, crosses international physical and financial borders with ease. Moneylaundering and narcotics trafficking in turn are leading to the stealthy corruption not only of law enforcement officers and court officials but also of entire governments. Added to this, fraud is becoming more prevalent and is increasing rapidly via the Internet where

unidentified, sophisticated hackers are breaking into banks, and equally sophisticated users are promoting scams of all kinds.

These new, disparate threats amount to a common danger to the economic base of states. They are admitted by states to be out of control The old sovereign methods of limited group defence and limited international information exchange which were effective against the Soviet Union, another limited group defence, are failing to deal with the absolute international dimension of these threats.

Moreover, the old methods of secret spying, disinformation, disruption and diplomacy which were used to fight the cold war are of little use in the fight against the new threats which are commonly based in criminal enterprise.

Crime is fought successfully by convicting the perpetrators or penalising them by way of civil or administrative proceedings, including sanctions.

Fighting crime, successfully, relies on information. First of all, gathering information which can be turned into evidence to support proceedings against suspects, both private and corporate. This information comes from public sources and secret sources, such as informants and electronic surveillance. This information must be shared not only amongst the various state agencies fighting crime but also internationally between such bodies and also between the juridical bodies supervising the prosecutions or other proceedings.

Information must also be disseminated to protect the public. Examples of this relate to threats to individuals at risk of physical harm, threats to financial institutions at risk of fraud and threats to corporations at risk of computer hacking.

Information has to be made available to independent oversight bodies to ensure that they effectively oversee the administration and operations of the law enforcement and intelligence agencies and others used in the fight against crime.

It is obvious that much of this information is information which states would wish to keep secret not only within their own separate agencies but also within their borders. However, the opacity of many of the threats and their international nature makes it imperative that state agencies share their information and share it across international boundaries. At the same time, full information must be divulged to oversight bodies. Secret

operations leading to the use of information as evidence in proceedings must be exposed to rigorous independent examination to prevent abuse of the juridical process.

States are, of course, used to such openness in dealing with ordinary crime. They are not, however, prepared for such openness when dealing with politically sensitive issues such as terrorism or the involvement of their secret agencies or the gathering of information by secret means. For instance information obtained electronically by the US NSA and the UK GCHQ is still not made available for court proceedings. It is essential that this information is brought into the law enforcement process as evidence. However, both the US and the UK are showing reluctance to engage these agencies in this duty.

This problem for states is being compounded by two other openness requirements that at present are only in their infancy. First, the nature of the new threats requires that states operate PR programmes to inform and educate the public at large. It is inevitable that information based on secret sources will form part of those programmes. Second, the public demand for information from the state will increase. The inability of states to control international crime will erode the quality of life within states. For example, society is already witnessing the gathering pace of indiscriminate terrorism including foreign hostage taking, juvenile drug abuse, fraud and the ghettoing of the wealthy and middle management into secure compounds. An increasingly educated society will increasingly demand to know why their quality of life is not being adequately protected by the state.

Thus, the phenomenon of the new information explosion, both by way of the international information highway and by way of the needs of law enforcement to control international crime, is opening secrecy like a knife into an oyster. The extent of the erosion is so deep that states are no longer capable of protecting their secrecy in the ways in which they have done in the past. And society is only at the threshold of this phenomenon.

The new information age will witness the increasing erosion of sovereignty as internationalisation develops. The concept of secrecy will diminish accordingly. It is difficult to predict the constituent elements of the concept at the point of absolute internationalisation, if that is ever reached. But the intermediate concept of secrecy is predictable.

To control secrecy in the first phases of internationalisation states must accept that old concepts of Cold War secrecy are dead.

A reassessment of what really needs to be protected is essential. That reassessment may not be easy. For instance, the US military in a recent US internal exercise found that their combat effectiveness was destroyed by the simple ability of the enemy to hack into the unprotected computers dealing with military supplies. Supplies were re-routed, countermanded or simply made to vanish by the enemy computer hackers. Chaos and defeat ensued. Of course, the answer to that problem lay not in making the supply system secret, but in protecting the on line system from hacking. A technical, not a secrecy, problem.

However, many areas of current secrecy are easily identifiable as being unnecessary and vulnerable in the new information age. For instance, education, public health and welfare are all areas where governments seek to create policies and administer certain provisions in secret. These are all societal problem areas where society is demanding increasing information.

By abandoning secrecy in these areas states will no longer have to protect against the depredations of information loss, save, of course, to protect the privacy of individuals. In doing so, states will free up administration and fiscal savings to protect what is vital to be protected in other areas.

Identification of other like areas of state business where secrecy is no longer viable or sustainable leaves few areas where a degree of secrecy remains necessary. Defence, foreign policy, intelligence, law enforcement (including immigration and customs) and commercial confidence (including research and development) are the obvious candidates.

However, these areas are all vulnerable to the new information age capabilities and demands. And by seeking to safeguard the whole area states incur huge costs with diminishing returns. Therefore, within each area it will be necessary to determine what is absolutely essential to be kept secret. The necessary physical and legal safeguards must then be constructed.

Secrecy within the intelligence and law enforcement area will require especially delicate balancing to ensure the protection of society on the one hand from the new threats and on the other from abuse by the state and its organs.

It should be noted that the protection should be afforded to society as a whole rather than to the state.

There are a number of reasons for this. In the fight against internationally based or executed threats the security of individual states becomes almost irrelevant. The fight has to be conducted on an international scale with resultant transborder intelligence and law enforcement operations and information exchange. The results of such operations will be enforced initially in whichever jurisdiction or jurisdictions become available or are most convenient. Gradually, as sovereign jurisdiction is seen to be unworkable to control international crime, jurisdiction will emanate from international tribunals, such as the International Criminal Court, or international regulatory bodies established for that purpose.

International organized crime is carried out in great secrecy. Secrecy that is enforced by bribery, physical assault and murder.

Intelligence operations are planned, covert, highly secret infiltrations into organisations which pose a threat to the state. The objective is to learn about the organisation and methods of the target. The operations use long term informants, telephone intercepts, eavesdropping devices and complex surveillance. They may take months or even years to penetrate a target and create a picture of its operations.

And the effect of this penetration on an illegal organisation is extremely damaging, whether by resultant court proceedings, disruption, exposure or discovery.

It is now accepted by the European Court of Human Rights in the cases cited above that secret intelligence operations may be used to protect society.

So just what are these intelligence operations?

They broadly fall into three categories Information and report; gathering information for the purpose of legal proceedings and disruption.

Information and report is obviously useful. It puts governments and others on notice and allows for strategic policy analysis and decisions. But, of course, it does not directly damage the criminal organisations.

Disruption is aimed at causing confusion, suspicion and panic. But not, of course, physical harm. On the other hand, neither do they sanction the

wrongdoer by, for example, imprisonment or relieving him of his powers to administer a company.

That is left to operations which gather information for the purpose of legal proceedings. Prosecution or civil administrative proceedings.

These operations must be led by the law enforcement or regulatory agencies. They are the overt arm, skilled in investigation. They are responsible for creating a case leading to proceedings.

Thus the intelligence agencies operate in very close co-operation with the law enforcement and regulatory authorities. Their purpose is to gather sufficient information about the activities of an organisation and its members so that evidence can be adduced in legal proceedings. Alternatively, the objective is to create a sting or entrapment operation against a predisposed criminal organisation and arrest the offenders in flagrante.

In either case there has to be a careful intelligence operation to gather as much information about the organisation as possible. Who are the leaders, who are the members, what criminal activity are they involved in, what are they planning, where do they get their money from. Where and how is that money laundered, who does the organisation associate with, why, are the associates aware, ignorant or just turning a blind eye.

This information is painstakingly gathered from informants, electronic intelligence and surveillance. Every move is covert. Every protection must be given an informant.

And these operations are carried out against organisations that are alert and have access to their own electronic counter measures.

It requires skill, patience and care.

But that is just the operational requirement.

The legal requirements are just as arduous.

The object is to convert the intelligence into useable evidence. Respecting the rules of evidence to the letter.

And that means that any activity or information discovered in an operation which may assist the defence in subsequent proceedings must be disclosed to the defence prior to trial.

But that activity and information includes secret activity and information, including the use of eavesdropping and informants. And it may be vital at the time of Court proceedings that such information is kept secret, particularly the identity of an informant. The whole proceedings must collapse if information relevant to the defence has to be kept secret. There is no alternative but to abandon the proceedings in those cases.

In the UK this problem is minimized by evidential procedures which open gateways for the intelligence to be put to the Courts as evidence. All the information gathered and the file of the operation is perused by prosecuting Counsel and then, in ex parte proceedings, by the judge. In these proceedings the judge can question why any information is deemed by the prosecution not to be relevant and request a justification for not releasing it to the defence. Documents may be passed to the defence in whole or redacted to protect sensitive non-relevant information.

The procedures are similar to the United States Classified Information Procedure Act Procedures. In fact, they were based on them.

It is no use going to Court hoping that vital secret information gathered in a lengthy intelligence operation will be ruled non relevant. That has to be worked out during the intelligence operation prior to any arrests. In the U.K. the intelligence agencies have lawyers working alongside the operational teams. They not only advise on the legal and civil rights issues in these operations but they also anticipate the relevance issues so that vitally secret sources do not become relevant at trial. This avoids not only any exposure of those sources but also, if they get it right, a trial having to terminate on a Judge's order that secret material is, in fact, relevant.

France and the Napoleonic Code countries have a similar but better Court Procedure. There, the examining judge discusses the balances of sensitivity and relevance with the agencies as the investigation progresses and prior to trial. He keeps two files, one for the Court and one confidential to him. Where he decides information is relevant he puts it on the court file. Where he decides it is secret but not relevant it goes on the confidential file and is not exposed in the proceedings.

Obviously in the intricacies of an operation it is surer to obtain the views of the judiciary at the time of the actual operational decision on relevancy than in limbo. As can be seen these decisions can lead to a failed prosecution. And the French system reduces this problem to a minimum.

The French system should become the international norm. It ensures that vital secrets are not exposed. It also ensures an ongoing oversight of the intelligence operations rather than post action oversight.

In this way the secrecy required by intelligence and law enforcement agencies to operate properly to secure convictions and regulatory penalties is secured. The judicial oversight will limit to a minimum the possibility of abuse in operations which result in judicial proceedings.

One draw back to the success of these operations and to information exchange generally is the shaky security of international information exchange between state agencies. The suspicions that jurisdictions harbour against each other about leakages, corruption or negligence prevent effective international information exchange. Interpol has not succeeded in defeating this problem. Nor has the recently established Europol.

The reason for this is that the problem is largely unspoken. And private channels of communication are established between individuals in various agencies. This is unsatisfactory not only because of the risk of misinformation but also of abuse.

States in the new information age must openly recognise the problem. Once they do, they will be able to open secure, limited personnel, single, cross border information exchange agencies. They will be formed of personnel with the highest security clearance, regularly vetted, using maximum encrypted communications. Of course, leakages will still occur and personnel may well succumb to the huge bribes on offer. But the leakages should be quickly traceable and defensive action taken in a timely manner. Much more so than pertains to the haphazard private communications that take place now. These agencies will gradually form the nucleus of international groups in organisations such as Europol and Interpol which will then succeed in broad crossborder secure information exchange.

It is self evident that the procedures outlined protect the agencies' operations with a great amount of secrecy.

That is vital as far as their operational work is concerned.

However, it is equally vital that society is assured that the state and the agencies are not abusing their powers in relation to what would normally be ordinary criminal investigations.

It is necessary to have PR to educate the public as to the new threats they face. It is equally necessary to have PR to educate the public as to how those threats are to be countered. If not, the public will resort to the tools of the new information age to find out for themselves. As has been ascertained the administrative efforts to contain wide field secrecy in the face of such a determined search will be prohibitively costly and patchily successful.

The depredations of international organized crime will become such that it will be necessary to assure society that the agencies are doing their job properly and that individuals in them are not being corrupted. In this respect, the policy and administrative details of the law enforcement and intelligence agencies must be made public.

States will, therefore, have to learn that the vital secrets of law enforcement and intelligence agencies that really need protecting are the identities of informants, the techniques employed in electronic surveillance, the details of ongoing operations and the identities of some of the members of the agencies. And even the latter must have regard to the increasing necessity internationally for witnesses to be identified.

But the problem of society's need to know will be such that it will be necessary to have an independent arbiter to decide what is and what is not a vital secret. Governments will no longer be trusted to take those decisions.

This leads to the second element of openness and that is oversight.

In a democracy the fount of information is Parliament. It is logical therefore that society will increasingly look to Parliament rather than any other body to oversee the policy, administration and operations of both the intelligence and law enforcement agencies in their work against international threats. Because the work will become more arduous it is also logical for Parliament to appoint an executive director with responsibility for administering oversight. The director's powers will have to be absolute in demanding information from the agencies as well as the public, save for the usual self incrimination limitations. The

director must also be able to roam among the files and interview members of the agencies as well as receive complaints from the public.

Public Reports would be issued, protecting only vital secrets.

In order to ensure public confidence to the fullest extent, the law enforcement and intelligence agencies must be brought within Freedom of Information legislation. The only limitation being a filter, logically through the executive director, to ensure that frivolous, time wasting enquiries are refused. The executive director would also make all decisions as to what are vital secrets, subject to Parliament's final decision.

These changes, taken as a whole, will allow states the best chance in the medium term successfully to defend both their vital secrets and also society from the challenges of the new information age and the internationalisation of serious crime.

In the longer term, as the new information age progresses, states will gradually turn to more international solutions to their problems.

Law enforcement and intelligence agencies will amalgamate. This will be necessary to focus better on the international nature of the threats. It will also become necessary to harness the escalating costs of running different agencies to combat the same problem.

The vital secrets will remain the same but overall secrecy in the area will diminish with the absence of inter-agency turf battles.

Moreover, the national agencies will gradually amalgamate to form one or more international agencies with special powers to deal with the threats to the international community. As a result relevant state secrets will become the secrets of the international agencies, with a further resultant diminishment of state secrecy in that area.

At the same time, oversight will gradually become internationalized. Either because it will be much easier and cheaper for one or more international organisations to oversee the international operations of multiple member national agencies or because international anti organised crime agencies will have already been established.

In either case state secrecy relating to the intelligence and law enforcement agencies will be determined by those international agencies.

This will result in harmonisation of secrecy and a corresponding diminishment of state secrecy.

In the new information age, society has the exciting challenge of the development of internationalisation. That challenge will be met in the face of the new enemy, the internationalisation of serious crime.

If states accept that secrecy must be diminished to a vital minimum then society will prosper. If not, state secrecy will be pierced by the needs of society and organised crime will plunder sovereignty.
DAVID BICKFORD CB