GENEVA CENTRE FOR THE DEMOCRATIC CONTROL OF ARMED FORCES (DCAF)

CONFERENCE PAPER

FREEDOM OF INFORMATION INTERNATIONAL TRENDS AND NATIONAL SECURITY

David Banisar

Deputy Director
Privacy International
and
Policy Fellow of the Open Society Institute
London, United Kingdom

Paper presented at the Workshop on " Democratic and Parliamentary Oversight of Intelligence Services", held in Geneva 3rd-5th October 2002, organised by the Working Group on the Parliamentary Control of Armed Forces (PCAF)and the Working Group On Democratic Control Of Internal Security Services (DCOIS) of the of the Geneva Centre for the Democratic Control of Armed Forces.

FREEDOM OF INFORMATION
INTERNATIONAL TRENDS AND NATIONAL SECURITY

DAVID BANISAR[1]

Access to government records and information is an essential requirement for developing and maintaining a civil and democratic society. Access facilitates public knowledge and discussion. It provides an important guard against abuses, mismanagement and corruption. It can also be beneficial to governments themselves – openness and transparency in the decision making process can assist in developing citizen trust in government actions. This is especially true for access to information about intelligence services and other national security bodies.

Governments around the world are increasingly making more information about their activities available. Nearly 50 countries around the world have now adopted comprehensive Freedom of Information Acts to facilitate access to records held by government bodies and over thirty more have pending efforts. While FOI acts have been around for several centuries, over half of the FOI laws have been acted in the last 10 years have seen the largest growth. The growth in transparency is in response to demands by civil society organizations, the media and international lenders.

However, there are still many problems as laws are weak or poorly implemented. Information about intelligence services is frequently withheld for national security groups in an overly broad manner that has little to do with protecting the state.

History of FOI laws

Freedom of information has been recognized for nearly 250 years. The world's first FOI law was Sweden's Freedom of the Press Act, approved in 1766. In 1789, the French Declaration of Rights of Man called for the right of citizens to review expenditures of the government. Over the years, access became more common to debates in Parliaments and the opening of most courts.

In modern times, Article 19 of the UN Declaration of Human Rights states:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Following the UNDR, countries slowly began to enact comprehensive laws for access to government-held documents and information: Finland enacted its law in 1951; the

---

[1] David Banisar is a Policy Fellow of the Open Society Institute and Deputy Director of Privacy International, a UK-based human rights group dedicated to advocating for privacy, free speech and freedom of information worldwide (http://www.privacyinternational.org/).

United States enacted its Freedom of Information Act in 1966; France in 1978; and Canada, Australia and New Zealand in 1982. The last ten years has been the most active period of countries adopting freedom of information laws. In Western Europe, only Luxembourg, Germany and Switzerland lack legislation and most Central and Eastern European countries have adopted laws as part of their transitions into democracies.

This trend is not limited to northern, industrialized countries. Nearly a dozen Asian countries have either adopted laws are or are on the brink of doing so. Pakistan approved a Freedom of Information Ordinance, 2002 just a few weeks ago. In South and Central America, a half dozen countries have adopted laws and nearly a dozen more are currently considering them. Africa is also catching up, South Africa enacted its law in 2001 and many countries in southern and central Africa, mostly members of the Commonwealth, are looking into following South Africa's lead.

In addition, countries have also adopted other laws that can provide for limited access including data protection laws that allow individuals to access their own records held by government agencies and private organizations, specific statutes that give rights of access in certain areas such as health or the environment, and codes of practices.

Factors for adoption

In general, civil society groups have played a key role in adoption of laws in many countries. This has included campaigning by press groups, environmental groups Governments are providing more as part of their “e-government” efforts to make services more efficient and accessible.

- Many new or recently revised constitutions include a specific right of access which required adoption of new laws. Over 20 countries now have constitutional provisions on access. Sweden’s Act is part of its Constitutional system. In Latin America, these provisions are knows as Habeas Data.

- International bodies such as the Commonwealth, Council of Europe and the Organization of American States have drafted guidelines or model legislation to promote freedom of information. The World Bank, the International Monetary Fund and others are pressing countries to adopt laws to reduce corruption and to make financial systems more accountable.

- Other longer-establish democracies are finally adopting legislation as a result of sustained campaigns by civil society and political scandals relating the health and the environment. This included Ireland, Japan and the UK.

- The expansion of the Internet in common usage has increased demand for more information by the public, businesses and civil society groups.

Problems

The mere existence of an act does not always mean that access is possible. In many countries, the access and enforcement mechanisms are weak or unenforceable. Governments resist releasing information, causing long delays or impose large fees,

courts uncut legal requirements and users give up hope and stop making requests. Independent bodies are weakened by lack of funds.

In some countries freedom of information laws are that in name only. In Zimbabwe, the Protection of Privacy and Access to Information Act sets strict regulations on journalists. In Paraguay, the law enacted restricted speech and was so controversial that media and civil society groups successfully pressured the government to rescind the Act shortly after it was approved.

A Brief Comparison of Laws

Overall there are many commonalities between the laws. In part, this is because only a few countries' laws have been used as models. The US FOIA has probably been the most influential law but Canada's and Australia's laws have been prominent with countries based on the common law tradition.

The most basic feature of FOI laws is the ability to ask for materials held by government departments. This is variously defined as records, documents or information. The definitions vary and in many laws led to gaps in access as computers replaced paper filing systems. Newer laws broadly define the concept so that there is little difference between them.

The right to request information is generally open to citizens, permanent residents and corporations in the country without a need to show a legal interest such as an injury that needs the information to remedy the harm. More recently adopted laws such as Ireland's and the UK's allow anyone around the world to ask for information. The US FOIA has been particularly used by newspapers and NGOs in countries where there is no Act to highlight the lack of information available in the country.

Access is generally limited to information which is already recorded down. Many Western European laws limit access to "official documents" which does not include drafts and other internal documents. Certain laws such as the Irish FOI require that department provide a written explanation of decisions that affect their interests and the Danish Act which requires authorities to record down information of importance. In some jurisdictions such as Austria and under the UK Code of Access to Information, the duty is only to provide information or answer questions, not to provide the original documents.

Which government bodies are covered

Generally the acts apply to nearly all major government bodies in the countries, except for the Parliament and the Courts. In some countries, the security and intelligence services are also exempt from coverage. In many parliamentary systems, documents that are submitted to the Cabinet for decisions and records of Cabinet meetings are also excluded.

An interesting development is the growing trend towards extending FOIA laws in countries to include non-governmental bodies such as companies and NGOs that receive public money to do public projects. This is frequently used to cover hospitals but could have broad affects and more basic government functions are outsourced to private entities. In South Africa, the law also allows individuals and government

agencies to obtain information from private entities if it is necessary to enforce people's rights. Thus far, there have been no cases on this issue but it is consistent with data protection acts and environmental regulations in other countries.

As international governmental organizations play an increasingly important role, the right of access to information must be codified in these new agreements. A key problem with access to information is that these organizations are based on a diplomatic viewpoint and thus limit access to information. Thus decisions that were once made on a local or national level where the citizen had access and entry into the process is now being made outside the country in a more secretive setting. Activists has constantly pressured organizations such as the WTO, the World Bank and the IMF to release more information. However, this is still limited. The EU's access regime is still more limited than that of most of the member countries.

Exemptions and balancing

There are a number of common exemptions that are found in nearly all laws. These include the protection of national security and diplomacy, personal privacy, commercial confidentiality, law enforcement and public order, information received in confidence, and internal discussions.

Many laws have provisions that require that a harm must be shown before the information can be withheld. The test for harm generally varies depending on the type of information that is to be protected. Privacy, commercial confidences, and national security tend to get the highest level of protection.

A number of countries' laws require that any exemptions be balanced against disclosure in the public interest. This allows for information to be released even if a harm is proven if "public benefit in knowing the information outweighs any harm that may be caused from disclosure." This is included in the Council of Europe's recommendations and is included in several laws including New Zealand, UK and Bosnia.

In many laws, factual information is frequently required to be released even when the full documents are exempted from release.

Appeals and oversight

A key feature of any act is how it deals with appeals from those who have had their requests for information denied. There are a variety of mechanisms for enforcing acts. These include administrative reviews, court reviews and enforcement by independent bodies generally referred to as information commissioners. The effectiveness of these different methods vary greatly. In general, the jurisdictions who have adopted an ombudsman or information commissioners appear to have greater openness. Ireland and New Zealand are frequently citied as having some of the most vigorous oversight systems.

The first level of appeal in most countries is the internal appeals. This typically involves appealing to a higher level in the department that the request was made to asking them to review the denials. This is of mixed utility. The experience in many countries such as Australia is that the internal system tends to uphold many of the denials and is used more for delaying releases than enhancing access.

Once the internal appeals have been completed, the next stage is an appeal to an external body. In some countries, such as Nordic ones but also Hungary and New Zealand and some Canadian provinces, appeal can be made to a Ombudsman, typically an officer of the Parliament. The Ombudsman generally does not have the power to make a binding decision but their decisions are considered to be quite influential and typically are followed by the government body. However, generally many Ombudsman are limited to handling specific cases and are not able to look more systematically at how FOI is working.

A more expansive approach that has been successful in many countries is the creation of an independent information commission, which can be part of the Parliament, the Prime Ministers' Office (such as in Thailand) or an independent body. In some countries such as Canada, France, Belgium and Portugal, these are independent bodies who just focus on FOI. The national Hungarian, and Canadian and German provincial models have combined the FOI commission with the national data protection authority. The new UK and Estonian laws also include this provision. In Ireland, the Information Commissioner is also the general Ombudsman.

An information agency can be tasked with many duties besides merely handling appeals. This includes general oversight on the system is working but also reviewing and proposing changes, training, and public awareness. In some countries such as Ireland and the UK, the Information Commissioner has the power to make binding decisions, subject to limited appeals or overrides by Ministers in certain cases.

The final level of review in most FOI laws is the courts. Most laws around the world allow the requestor to appeal to the either specialized courts such as the Administrative Appeals Tribunal or the national courts. The courts can obtain copies of most records and make decisions. Depending on the procedure needed to gain access and the scope of the review, the utility of the courts vary. In some countries, the court can only review a point of law once a tribunal decides.

A less efficient system is where the courts serve as the only external point of review, such as in the United States. This effectively prevents many users from enforcing their rights because of the costs and significant delays involved in bring cases to courts. The courts are also generally deferential to agencies, especially in matters of national security related information.

Duty to Publish Information

Another common feature in FOI laws is the duty of government agencies to routinely release certain categories of information. These typically include information on the structure of the organization, its primary functions, a listing of its top employees, annual reports, and other information. Newer FOI laws tend to proscribe a listing of information, except in the UK, where the Information Commissioner can issue a model publication scheme and must approve each entities' scheme (over 70,000).

One problem is how to ensure adequate dissemination of that information. Electronic networks is one possibility. In the United States, the Electronic Freedom of Information Act promotes the disclosure of records in electronic form. This leaves the possibility of not only providing for more efficient, quick access, but also new ways of using information such as using transactional records and geographic information

systems to analyze government records in new ways. In Estonia, the FOI requires each public body to maintain a web site and includes a long list of information that must be on each site.

The records can also be used for new purposes. In Canada, Professor Al Roberts of Syracuse University uses the Access to Information Act to obtain the logs of requests in electronic form puts them up on the net to allow people to see what requests are being made so that they can obtain the records themselves. Prof. Roberts also uses the records to analyze how the different departments respond to requests. In the US, the Transactional Records Access Clearinghouse (TRAC) obtains the electronic records on all federal criminal cases and merges that data with other information such as census records to analyze the workings of the criminal justice system in the US. The information is put up in a searchable web-based system that is open to the media, civil society groups and others. In Norway, all documents are indexed when they are received or created and the index is made available on the Internet.

National Security and Freedom of Information

As noted above, freedom of information laws typically include an exemption for information relating to national security. Many countries, especially those in the Commonwealth, also have Official Secrets Acts which set limits on the release of information and criminalize its unauthorized release.

The scope of this exemption varies. In some countries such as the UK, the intelligence agencies are excluded completely from coverage under the FOI acts. In other countries, the national security information is presumptively kept secret. Even when there is oversight, such as in the US, the courts are deferential to the agency decisions. These broad exemptions to access frequently raise serious concerns about the role of intelligence agencies, including some of the most long-standing democracies. Ensuring national security is important to all nations but the balance is frequently skewed.

Not all countries take this approach. A few countries allow access to some information balanced against harm such as the new Bosnian law which requires “substantial harm.” In Mexico, information relating to “the investigation of grave violations of fundamental rights or crimes against humanity” may not be classified and all departments must produce a regular index of all classified files, which is made public. Other make the decision subject to review by a commissioner, ombudsman or court. In Hungary, under the Secrecy Act of 1995, the Parliamentary Commissioner for Data Protection and Freedom of Information is entitled to change the classification of state and official secrets. In Peru, journalists and senior military officers met and agreed to common definitions of national security and the types of information that could be withheld.

Following the transition to democracy, many countries have adopted laws to make available the files of the former secret police forces. These files are made available to individuals to see what it being held on them. In other countries, the files are limited to “lustration” committees to ensure that individuals who were in the previous secret services are prohibited from being in the current government or at least their records are made public. Prior to reunification, East Germany made its files widely available

not just to individuals who were victims but also to journalists and historians. The Czech Republic recently amended their act to allow for broad access.

Problems with Secrecy

The problem arises when these exemptions are used to hide embarrassing or even silly facts rather that dealing with the core information necessary to protection national security. Supreme Court Justice Potter Stewart said in the Pentagon Papers case, "When everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion." In the UK, the 1911 OSA, which was not revised until 1989 and is the basis for many secrets laws, created 2,000 criminal offenses including the release of information on the number of cups of tea consumed in the cafeteria of the Security Service. In Malaysia, Parliamentary opposition leaders are currently under investigation after obtaining a copy of the state budget two days early which allowed them to come up with an alternative version, embarrassing the government.

It is also used to hide abuses and corruption, such as interference in the domestic political system and against government opponents by intelligence and law enforcement agencies. The UK prohibits individuals, including those who are currently ministers and members of Parliament, from accessing their security files from when they were student protestors in the 1970s because of their fear of showing how pervasive the surveillance was at the time. Following the horrific events of September 11, authorities in the United States on the national and state level have been US has been extensively cracking down on access to information using security as a justification. This has included an Executive Order that discouraged discretionary releases, the removing of information from agency web sites and ordering the destroying of CD-ROMs and the closing of court hearings. Information on the use of the Patriot Act have been kept secret, even from the Congressional committees that are empowered to oversee its use.

This approach has not been followed worldwide. Following September 11, only Canada made changes to its FOI law to limit access. Germany dropped its limited efforts to enact a law and the UK announced a significant delay but both of those are due to opposition by the internal bureaucracies rather than terrorism. Jamaica, Mexico, Panama, Peru, Romania and the sub-national jurisdictions of Scotland and Delhi, India have all enacted new comprehensive laws to allow for citizen access to government information and dozens of other countries are in the process of doing so. A number of countries in Eastern Europe have also opened up the archives of the Soviet-era secret police, making it easier to get info out of the files about abuses from that era.

Another troublesome area is the new acts on the protection of classified information. Many countries in Central and Eastern Europe have been adopting these acts as part of the process to joining NATO. NATO has thus refused to provide a copy of the draft legislation that they are requiring the countries to adopt. The laws frequently apply a very restrictive view of the disclosure of information that goes beyond files from NATO. In Bulgaria, the law eliminated the Commission on State Security Records which regulated access to, and provided procedures for, the disclosure and use of documents stored in the former State Security Service, including files on government

officials. The EU has also adopted new restrictive NATO regulations on protection of all security information held by the EU that are currently being challenged in court by the European Parliament.

The use of secrecy also creates significant costs. The US Information Security Oversight Office estimated in 2000 that the annual cost of creating and maintaining secrets was $4.3 billion, not including the costs of the Central Intelligence Agency.

The Johannesburg Principles

In 1995, a group of experts in freedom of speech and information met in Johannesburg, South Africa to try and facilitate a greater debate on properly defining the scope between national security and access to information. The group developed principles that were released in 1996 and were subsequently endorsed by the OAS Special Rapporteur on Freedom of Expression, OSCE Representative on Freedom of the Media and UN Special Rapporteur on Freedom of Opinion and Expression in 2000.

The relevant provisions on access to information state:

> **Principle 11: General Rule on Access to Information**
> Everyone has the right to obtain information from public authorities, including information relating to national security. No restriction on this right may be imposed on the ground of national security unless the government can demonstrate that the restriction is prescribed by law and is necessary in a democratic society to protect a legitimate national security interest.
>
> **Principle 12: Narrow Designation of Security Exemption**
> A state may not categorically deny access to all information related to national security, but must designate in law only those specific and narrow categories of information that it is necessary to withhold in order to protect a legitimate national security interest.
>
> **Principle 13: Public Interest in Disclosure**
> In all laws and decisions concerning the right to obtain information, the public interest in knowing the information shall be a primary consideration.
>
> **Principle 14: Right to Independent Review of Denial of Information**
> The state is obliged to adopt appropriate measures to give effect to the right to obtain information. These measures shall require the authorities, if they deny a request for information, to specify their reasons for doing so in writing and as soon as reasonably possible; and shall provide for a right of review of the merits and the validity of the denial by an independent authority, including some form of judicial review of the legality of the denial. The reviewing authority must have the right to examine the information withheld.
>
> **Principle 15: General Rule on Disclosure of Secret Information**
> No person may be punished on national security grounds for disclosure of information if (1) the disclosure does not actually harm and is not likely to harm a legitimate national security interest, or (2) the public interest in knowing the information outweighs the harm from disclosure.

Principle 16: Information Obtained Through Public Service
No person may be subjected to any detriment on national security grounds for disclosing information that he or she learned by virtue of government service if the public interest in knowing the information outweighs the harm from disclosure.

Principle 17: Information in the Public Domain
Once information has been made generally available, by whatever means, whether or not lawful, any justification for trying to stop further publication will be overridden by the public's right to know.

Conclusion

The current trends on access to information is both positive and worrying. On the one hand, many countries are becoming more open. On the other hand, important decisions are consistently moving towards international organizations which have resisted becoming more transparent.

Effective oversight of intelligence services requires that information about their activities be made public. Many countries have an overly expansive view of national security that has little to do with ensuring the integrity of the nation. These laws and restrictions need to be reviewed.

Established in 2000 on the initiative of the Swiss government, the Geneva Centre for the Democratic Control of Armed Forces (DCAF), encourages and supports States and non-State governed institutions in their efforts to strengthen democratic and civilian control of armed and security forces, and promotes international cooperation within this field, initially targeting the Euro-Atlantic regions.

The Centre collects information, undertakes research and engages in networking activities in order to identify problems, to establish lessons learned and to propose the best practices in the field of democratic control of armed forces and civil-military relations. The Centre provides its expertise and support to all interested parties, in particular governments, parliaments, military authorities, international organisations, non-governmental organisations, academic circles.

Geneva Centre for the Democratic Control of Armed Forces (DCAF):
rue de Chantepoulet 11, P.O.Box 1360, CH-1211 Geneva 1, Switzerland
Tel: ++41 22 741 77 00; Fax: ++41 22 741 77 05
E-mail: info@dcaf.ch
Website: http://www.dcaf.ch