MAKING DEMOCRACY WORK

The Media Tool Box 4

Access to Information

Christel and Hendrik Bussiek

fesmedia Africa

Content

1. About this Box

Access to information is widely acknowledged as a basic right of citizens in a democracy. And the need for appropriate legislation to give shape and meaning to that right has been a fashionable topic of debate for some time now - not just in the media fraternity but equally among lawmakers and civil society as a whole. The important thing - as with all fashions - is to separate the hype from the substance and decide what is really wearable in everyday life. In practical terms: what information are we talking about, what exactly does the right to access entail and how can it be framed in a law in a useful and practicable manner?

Information, of course, is a hold-all term and a lot of it is there in our faces all around us (sometimes more than we can stomach) or easily available to anyone who cares to look for or notice it. Some of it is private and should remain so, even though many might find it interesting to know. Access to information does not mean ignoring the right to privacy or opening the door to unbridled curiosity, an army of peeping Toms in the guise of citizens exercising a legitimate right. What we are dealing with here is information of general concern but held

exclusively by some only and not freely accessible to all.

Typically this is information held by governments and public bodies, gathered in the course of and for the purpose of their work - and jealously guarded from public scrutiny. Citizens all over the world are familiar with this tendency of those in authority and Africa is certainly no exception when it comes to this truly international culture of secrecy. (Why are bad habits always the easiest to share, one wonders.)

The unwillingness to release information on the part of authorities and their attempts to hide behind so-called official secrets regulations indicate a fundamental misunderstanding of the nature of their job and their mandate. In a democratic state, citizens choose to task some in their midst to run the affairs of the state on their behalf - by voting for politicians and paying for public servants. Any information acquired or generated by government and public bodies while discharging the duties they have been assigned, therefore, is public property and belongs to all citizens. Access to it is not a privilege, to be granted or withheld, but a right.

From the early nineties of the last century, governments around the world have increasingly acknowledged this right. More than forty countries now have legislation in this regard; more than thirty are in the process of developing it, bearing in mind what the Special Rapporteur of the United Nations on Freedom of Opinion and Expression wrote in 1995:

> "Freedom will be bereft of all effectiveness if the people have no access to information. Access to information is basic to the democratic way of life. The tendency to withhold information from the people at large is therefore to be strongly checked."

It all began with the collapse of dictatorships and authoritarianism in the late 1980s. New democracies emerged, such as those in Southern Africa or in central and eastern Europe, and adopted new, progressive constitutions that include guarantees of the right to information. Older democracies followed the example of the new kids on the bloc. Today in Europe, for example, Switzerland is the only country not to have access to information legislation - all others have either adopted such acts or are in the process of doing so.

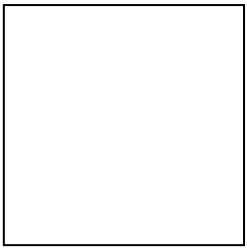
Of course, the right of access to information applies equally to all citizens. In practice, it will probably be exercised most often by non-governmental organisations and by the media on their behalf. Journalists in their day to day work are the most likely to experience what it means to run into or try to overcome the wall of secrecy erected by officials reluctant to part with 'official' information. Little wonder then that, together with civil society as a whole, they have been in the forefront of the fight for the realisation of the right of access. As early as 1992, journalists from all over Southern Africa resolved in a Declaration of Lusaka (Zambia):

> "There shall be a statute guaranteeing the right of freedom of information for all citizens which

> the state shall be obliged to comply with, except when the state is able to prove in a Court of Law that the release of such information would endanger the security of the nation; such Freedom of Information Acts shall replace all Official Secret Acts."

More than a decade later there is still a lot of ground to cover to get there - but the wall is definitely crumbling. What the Declaration refers to broadly as an acceptable exception - withholding of information that "would endanger the security of the nation" - is now being much more narrowly and precisely defined. There is an existing body of law in various countries and a wealth of experience gained with the ways to actually make access to information work.

This Tool Box is meant to help keep up the pressure on the authorities not just to pay lip service to the idea of free access to information but to implement it. It will describe in some more detail why such access is an essential citizen's right and how it can be exercised efficiently, without compromising other rights or legitimate concerns in the process. It will also look at those pieces of existing legislation that need to be reviewed to ensure open and transparent government.



2. Why the right to access to information?

Information is needed in order to make decisions - on individual matters, on community issues and on matters of state. The more people any decision is likely to affect, the more important it is for all the relevant information to be shared as widely as possible, even more so when such decisions are to be made by some on behalf of others. Representative, democratic governance can only function when all have equal access to the facts and are thus able to play an equal part in the decision making process.

Openness, transparency, accountability - all these popular buzzwords of contemporary political discourse will remain empty promises if there is no free access to information. Citizens need to be informed for them to be able to form an opinion and express their views on the affairs of the state. And they need to be informed for them to be able to judge how successfully - or otherwise - the authorities are dealing with them. Unless they have

unhindered access to information they can not hold them accountable for their performance.

Once again: issues of governance are not the preserve of the authorities, for them to deal with at their discretion. ‘Affairs of the state’ - be they organisational matters, reforms to be initiated, priorities to be set within the available budget, or decisions on the future of public health care or education - are the citizens’ very own affairs, all of them affecting their daily lives in one way or another. In a democratic state, both the governed and the government, on the basis of shared information, must work together to find and decide on the best way forward.

This is especially true in developing countries. It is now generally agreed that the development process can only be successful if it is actively supported by a strong civil society. And for this support to be gained, the authorities need to lay open all the available facts, projections and possible alternatives. After all, they are in possession of all this relevant information not because of their superior wisdom but because they collected it in the course of their duties as mandated by - and at the expense of - the tax paying public.

Not infrequently, it is argued that only well educated people in a country with high standards of living can afford the ‘luxury’ of taking part in such open decision making processes and are able to understand the complicated issues involved. This is an arrogant and self-serving argument used by authorities of the old order unwilling to allow

democratic checks on their powers. And it is certainly not true in the African context with its long standing tradition of consultation and extended deliberations in the community where everyone will have their say before decisions are taken. Access to information and economic development feed into each other: The more information people have, the more will their motivation for change spur on development.

Be it with regard to development or any other policies to be undertaken, and perhaps even more so to the performance of public bodies, citizens should not have to rely on information provided voluntarily. In some countries, Botswana being one example, governments point to the fact that they have set up a system of press officers in the various departments whose job it is to deal with requests for information both from the media and the general public. But this is a far cry from properly instituted access to information mechanisms. The information issued by such officials is bound to be more of the PR variety - material to show up successes and generally make the authorities appear in a good light. That may be a legitimate purpose but it is not what the public need most in order to assess their performance and hold them accountable.

All too often officials and politicians also 'leak' selected information to the media for their own purposes - to influence a decision making process, to damage the reputation of a competitor or simply to boost their ego. Journalists, also all too often, will jump at the chance of a scoop and publish the information, quoting 'authoritative sources'. Citizens,

including journalists, need access to the full facts of a matter to prevent the propagation of half-truths and slanted, one-sided stories.

Access to information, then, needs to be acknowledged as a right, not as a privilege, and it can not be up to the authorities themselves to decide what they want to disclose and deem fit for public consumption. The public must have the right to request in particular the controversial or unfavourable material, preferably hidden in secret files because it is likely to damage the positive image to be projected or runs counter to declared intentions or pet projects - critical financial or environmental assessments of planned developments by independent bodies, internal reports on shortcomings in government departments and the like. And the public needs just this sort of information not because it makes good headlines or to lambaste government for its failures, but because it concerns them: bad and inefficient governance affects their lives and well-being. On a positive note: Once the public knows the full facts of a matter and can bring pressure to bear on the authorities it will be possible to reverse bad decisions and thus prevent harm.

The other type of information that all citizens need to be able to access freely is personal information: all kinds of data on them held by the authorities. These may range from their health or financial status and employment or police records to internal reports on their political or social activities. Regardless of whether there may be a legitimate purpose for such

data to be compiled, every citizen has the right to know what they are and whether they are correct.

Civil societies and governments on the continent wishing to develop comprehensive access to information legislation do not need to start from scratch. The African Commission on Human and Peoples' Rights in its 2002 Declaration on Freedom of Expression gives a clear and bold guideline on the issue:

1. Public bodies hold information not for themselves but as custodians of the public good and everyone has a right to access this information, subject only to clearly defined rules established by law.
2. The right to information shall be guaranteed by law in accordance with the following principles:
    - everyone has the right to access information held by public bodies;
    - everyone has the right to access information held by private bodies which is necessary for the exercise or protection of any right;
    - any refusal to disclose information shall be subject to appeal to an independent body and/or the courts;
    - public bodies shall be required, even in the absence of a request, actively to publish important information of significant public interest;

- no one shall be subject to any sanction for releasing in good faith information on wrongdoing, or that which would disclose a serious threat to health, safety or the environment save where the imposition of sanctions serves a legitimate interest and is necessary in a democratic society; and
- secrecy laws shall be amended as necessary to comply with freedom of information principles.

3. Everyone has the right to access and update or otherwise correct their personal information, whether it is held by public or by private bodies.

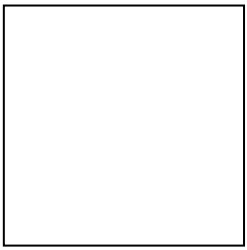
The South African constitution of 1996 provides for the right of access in its section 32:

> (1) Everyone has the right of access to –
>
> (a) any information held by the state, and
> (b) any information that is held by another person and that is required for the exercise or protection of any rights.
>
> (2) National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state.

Because lawmakers in South Africa had to give their attention to a lot of other areas, but also because of the specific intricacies of the matter, it then took

another four years before the required act was actually passed by parliament in 2000. This is now regarded as the most progressive piece of legislation in its field worldwide. Nevertheless, experience over the past few years points to a number of problem areas worth looking at more closely in order to arrive at more workable solutions. Another African document that could form a basis for discussion is the Zambian Access to Information Bill, tabled in parliament in 2002 but not yet passed into law.

We will go through the issues step by step, using these and other pieces of legislation and documents, to see how such provisions can best be crafted and what pitfalls should be avoided.



3. Who should be obliged to give access to information and to whom?

So far we have talked in a very general sense about the "government" or "the authorities" as being obliged to release information. Most legislation refers to "public bodies" or "public authorities", intentionally broad terms that encompass any part of government: parliament (the legislative), ministries/departments (the executive) and courts of law (the judiciary) at all levels (national, regional and local). The category also includes institutions that are owned, controlled or substantially financed by funds provided by the state (public corporations or parastatals), or that carry out a public function on behalf of a public authority (such as maintaining roads or operating railway lines). All these public bodies should be obliged by law to disclose information on request by a member of the public.

That is the understanding worldwide. Both the African Commission's Declaration on Freedom of Expression and the South African Promotion of Access to Information Act go one step further than most international precedents. They demand or grant a right to access also to information held by

“private bodies” if that information is necessary “for the exercise or protection of any right(s)”.

A private body, according to the South African act, is any “person” who carries on, or once carried on a trade or business or profession. A Model Freedom of Information Law presented by the international advocacy organisation Article 19 in 2001 defines such a “private body” as “any body … that … carries on any trade, business or profession, but only in that capacity; or has legal personality”.

This is where things get a little more difficult. It is probably easy to agree that information necessary to protect a right or to prevent harm should be released - though exactly what would qualify as such will be open to interpretation. But can private bodies simply be subjected to the same legal obligations as public ones? Does the right to privacy not also apply to private businesses, and what about the legitimate need for confidentiality so that a company can keep its competitive edge over its rivals in the field? And should the law apply equally to all kinds of enterprises, to big banks and insurance companies just as to the medium sized manufacturer, the medical centre or law firm, to the family business with a handful of employees or even the corner shop? Should the line of business a company is in be taken into account – should those dealing with environmentally sensitive products or arms, for example, be more subject to public scrutiny than others? How and where to draw the line?

These are tricky issues and satisfactory answers have not yet been found. The South African experience, so far, indicates that the inclusion of private enterprises in the act was probably over-ambitious and does not work in its present form. On a very pragmatic level: such an approach is also hard to lobby for and those pushing for the right to access should perhaps rather keep their eyes on the big prize. It will be difficult enough to convince public authorities that they have a democratic obligation to grant access to their documents and files. Taking on Big Business at the same time or getting bogged down in minute detail of what are really side issues will make the task even be more complicated. Instead of going for the full Monty all at once one should perhaps concentrate on the job of drilling the first and strategic holes into the wall of secrecy surrounding state affairs.

A section in an access to information law defining bodies obliged to disclose information could then read as follows:

> "Public body" means
>
> (a) any part of government or government institution as defined by the constitution (legislative, executive and judiciary) at all levels from national to local;
>
> (b) any body appointed or established by law to carry out a public function;
>
> (c) any body either owned or controlled by a public authority as defined under (a) and (b); or

(d) private bodies which carry out public functions on behalf of a public body as defined under (a) and (b).

What precisely will these bodies have to disclose? What is “information”? The short answer in this case is: everything - all material that they collect, produce or keep on file in the course of their work. This will either be in paper form or, increasingly, stored on computer data bases. Information could also be kept on sound tapes or videos. The definition of “information” in a law should therefore be as broad as possible:

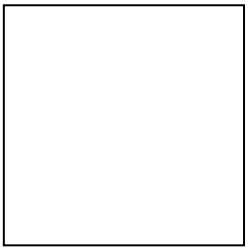
> “Information” means any material regardless of form or medium in the possession or under the control of a public body.

Who should have the right to request access to information? As pointed out earlier, this will be the right of every individual citizen and not just specific groups or the media. Some countries even allow foreign nationals the right of access to public records.

The law should also include the provision that a requester - the person asking for information - will not be obliged to give any reason for the request. There may be exemptions regarding the kind of information to be released, but the right of access as such is unconditional and, like all basic rights, can not be denied. Making it dependent on “good reasons” would make such denial a matter of

subjective interpretation - in effect it would mean opening the door for all kinds of feeble excuses. The South African Act, for example, says explicitly that “a requester’s right of access … is … not affected by any reasons the requester gives for requesting access”. Other legislators say that “the body shall neither require nor ask for any reason or justification for the request”.

When it comes to disclosure by private bodies, the situation would be slightly different: Since the demand for information in that case must be based on the condition that such information is necessary for the exercise or protection of a right of either an individual or a community, some reasonable arguments should be provided by the requester that this condition is likely to be met.



4. Who should be in charge of disclosing information?

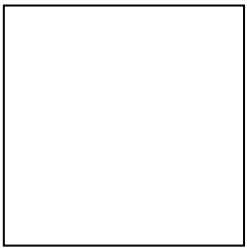
The aim should be to make it as easy as possible for citizens to obtain the information they are interested in. For this reason many acts oblige public bodies to put in place an “information officer” in charge of receiving and dealing with requests from the public. This will not necessarily be a public servant or employee exclusively designated for such duties. As is the case in South Africa, this could be the “Director-General, head, executive director or equivalent officer” of a public body.

Still on the question of user-friendliness: The South African law also requires all public bodies to develop a “manual” containing all the relevant information that interested citizens may need - a description of the structure and functions of the body, address and contact details of the information officer, and categories of records available without even having to request access to them under the act. From that material the Human Rights Commission then compiles a complete “guide” on all public bodies.

As in every bureaucratic decision there must be a way for citizens to appeal if a request is turned down and access to information refused. The first and obvious port of call is a court of law - the option chosen in South Africa. This, however, is a very costly and time-consuming route to go and this provision is now regarded as one of the major flaws in the South African legislation. Other countries have designated the Ombudsman - where such an institution exists - to act as an appeal body, or, alternatively, the Human Rights Commission. One could also establish a special Public Information Commission similar to the one envisaged in Zambia for example. There, a bill - still under consideration - provides for such a Commission to be appointed by parliament, one of its tasks being to review decisions by public bodies or even impose fines against officials who do not comply with the law. The Zambian Commission is to consist of one nominee from the Law Society (to ensure legal expertise), and two members each nominated by media organisations and civil society groups. Another option, as suggested by Article 19, is to appoint one person as a Public Information Commissioner to arbitrate where requests have been denied.

For the sake of even easier access, one might consider using such a Commission (or Commissioner) as the central port of call for all requests for disclosure of information from the public. An ordinary citizen may find it difficult to identify the body or department in charge of the desired information, and requests could end up being shifted from one to the other. Having one centralised body would make for a more efficient

procedure. It would also help save time for information officers or make them redundant altogether: The Commission/er would pass a request on to the appropriate head of department who would then task a member of his staff to compile and release the information to the Commission. In this way, the Commission would be able also to monitor whether the body in question is indeed responding satisfactorily and timeously.



5. Should all information be equally accessible?

This question is easily answered with regard to personal information. Of course, all citizens have the right to know what data on their individual circumstances the authorities have on file. More than that: if they find that these data are not correct, they have the right to demand that they be corrected. A number of young democracies, for example Bosnia and Herzegovina (South East Europe) have introduced provisions accordingly. The appropriate article could read:

> 1. Every person has the right to ensure that his or her personal information in the control of a public body is correct, current, complete, relevant to the legitimate purpose for which it is held, or not otherwise misleading.
>
> 2. If the conditions outlined under (1) are not fulfilled, every person has the right to request
>
> > (a) an amendment to the information in question, or
> >
> > (b) a comment that shall be appended to the personal information.

3. Amendments and the inclusion of comments shall be free of charge.

With regard to all other kinds of information, the question of unqualified access is the most vexing of all problems to be solved in legislation of this kind. The dilemma which needs to be acknowledged and confronted squarely at the outset is that not even the most transparent state can afford to disclose all the information at its disposal. A state prosecutor cannot be forced to reveal the kind of evidence he has against an accused before the case comes to court. The revenue service should not be allowed to disclose the income of individual tax payers to third parties. The Defence Force will not hand out details on its strategic plans to anyone who cares to ask. Ministries will rightly refuse to give access to first drafts of a new policy before it is ready for public debate. All these and many other cases must be taken into account when framing a good law: not an ideal wish list, but a set of provisions that will stand the test of real life.

A workable access to information law, then, will have to contain exemptions or exceptions from the rule of disclosure. And, contrary to popular gut feeling and at first glance paradoxically, it is likely to be a better law if it lists more rather than less such exemptions. The reason is simple, really, and takes us back to the point of departure for any such law: Governments and public bodies generally tend to hold on to the information they have rather than share it willingly. So any exemptions they may claim must not just be named at the outset, but also be

clearly and narrowly defined so that they can not be used as loopholes or easy excuses for non-disclosure. With exactly this in mind, the Act on the Openness of Government Activities in Finland, to name just one, lists no less than 32 classes of documents that may not be disclosed.

Take the issue of national security, for example. What if a law merely said (as some do): disclosure of information may be refused if it "would cause serious prejudice to the defence or national security"? This leaves wide room for interpretation and would allow the Ministry of Defence and the like almost unchecked discretion to claim such possible danger and thus decline to release any but the blandest information in their possession. Such imprecise language in the law would defeat its very purpose.

The general rule - as with all lawful restrictions placed on rights and freedoms - is that the exemption of any information from disclosure must be necessary, justifiable and proportionate in a democratic society. The following list is based on several pieces of legislation worldwide, from Sweden - the oldest such law - to South Africa and the young democracies in South East Europe, as well as on recommendations by Article 19.

Protection of privacy

All governments - like it or not - collect heaps of personal information on their citizens. This is kept in tax files, police files, records in the possession of the education department, the traffic department

and so on. When responding to requests for disclosure, the right to privacy of individuals needs to be protected. Such records are a matter between the individual citizen and the authorities and do not concern any third party. Other citizens do not have the right to access them. Such personal information could be defined as - and these examples are taken from the South African act - information relating to gender, national, ethnic or social origin, race, marital status, pregnancy, sexual orientation, age, physical or mental health, disability, religion, belief, culture, language and birth of the individual; information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved; as well as correspondence sent by the individual which is protected by the constitution (privacy of mail). Therefore the first exemption could read:

> Disclosure of all or part of the information requested must be refused if it would involve the unreasonable disclosure of personal information about a third party.

There should, however, be one exemption from this exemption - or rather a necessary clarification. If a journalist, for example, follows up a story on allegations of corruption against a civil servant, such a person should not be able to hide behind this privacy provision. An additional clause will provide for that:

> Access to the information must not be refused if it consists of information about an individual who

is or was an official of a public authority and which relates to the position or functions of the individual.

Protection of commercial interests

Government departments have in their possession a lot of information on businesses and their products or services, collected for example during tendering processes. Obviously, such information should not be allowed to fall into the wrong hands, in particular those of competitors. Most acts provide for the protection of commercial interests along these lines:

> Disclosure of all or part of the information must be refused if it consists of
>
> (a) trade secrets, or financial, commercial, scientific or technical information of a third party; the disclosure of which would be likely to cause harm to the commercial or financial interests of that party; or
> (b) information supplied in confidence by a third party, the disclosure of which could reasonably be expected to cause harm to a third party in commercial competition or in contractual or other negotiations.

Again, there should be one important exception. The claim to commercial confidentiality must not be used to conceal potential dangers or risks from the public. Citizens must retain the right of access to any information or records held in that regard:

Access to the information must not be refused if it consists of information about the results of any product or environmental testing or other investigation conducted by a third party and its disclosure would reveal a serious public safety or environmental risk.

Protection of safety of individuals and property

This is another fairly obvious exemption. No sensible person will expect a public body to disclose details of security arrangements for its buildings or personnel, for example. The respective section could read as follows:

Disclosure of all or part of the information must be refused if it

(a) could reasonably be expected to endanger the life or physical safety of an individual; or

(b) would be likely to cause harm to

(i) the security of a building, structure or system (including computer or communication systems), a means of transport, or any other

property; or

(ii) methods, systems, plans or procedures for the protection of an individual, the safety of the public, or the security of property.

Protection of defence and security

As was pointed out before, the security of the (democratic) state, in other words: the security of all citizens, is a valid concern. People rely on the authorities to provide that protection and therefore need to accept that this will entail some limitations to their right of access to information. A general provision in this regard might say:

> Disclosure of all or part of the information may be refused if access to that information could reasonably be expected to cause harm to the defence and security of [name of country].

This wording by itself, of course, is still too broad. If the state, for example, enters into a major arms deal, citizens/taxpayers will have a legitimate interest to look into the various tenders and their relative merits. The authorities should not be allowed to evade perhaps uncomfortable scrutiny of their decisions by summarily refusing disclosure “in the interest of national security”. Possible exemptions under this heading should therefore be more clearly specified:

> Information contemplated here includes information

(a) relating to military and security tactics or strategy;

(b) held for the purpose of intelligence relating to defence.

Protection of international relations

There are some parallels here with the accepted need for protection of personal information exchanged between two parties against unwanted or unauthorised disclosure to a third party. International relations are similarly conducted on the basis of mutual trust. The understanding is that the content of verbal or written communication between state officials is not generally a matter for public consumption (unless otherwise agreed), and that each side will respect the other's sensitivities and concerns in this regard and honour the principle of confidentiality. This international consensus should be reflected in the law:

> Disclosure of all or part of the information may be refused if access to that information could reasonably be expected to cause harm to the international relations of [name of country] because it
>
> a. is information supplied in confidence by or on behalf of another state or an international organisation,
>
> b. is required to be held in confidence by an international agreement or customary international law.

c. deals with the positions adopted or to be adopted by [name of country] for the purpose of present or future international negotiations;

d. constitutes diplomatic correspondence exchanged with another state or an international organisation or official correspondence exchanged with diplomatic missions or consular posts in [name of country].

Protection of economic interests of the state

As in the case of private businesses, the economic interests of a state also deserve protection:

> Disclosure of all or part of the information may be refused if it consists of
>
> (a) trade secrets, or financial, commercial, scientific or technical information of the state, the disclosure of which would be likely to cause harm to its commercial or financial interests; or
>
> (b) information, the disclosure of which could reasonably be expected to prejudice the state in contractual or other negotiations.

Again, as with the protection of private commercial interests, the same exemption from the exemption applies:

Access to the information must not be refused if it consists of information about the results of any product or environmental testing or other investigation conducted by a third party and its disclosure would reveal a serious public safety or environmental risk.

Protection of law enforcement and legal proceedings

The right of access to information does not override the need for the police and the judiciary to get on with the job of law enforcement – in order to protect the safety of all citizens and in accordance with the law and their regulations. It must be understood that these agencies will not disclose certain information: the names of minors in custody or under investigation, for example, details of planned arrests of suspects, of ongoing criminal investigations or the strategy of the prosecution in an upcoming court case.

Disclosure of all or part of the information must be refused if access to that information

(a) is prohibited in terms of the Criminal Procedure Act; or

(b) would jeopardise law enforcement and legal proceedings.

Protection of deliberative processes

This is a very relevant provision to make especially in an open and democratic society. Policy development is a consultative process carried out by way of communication, that is the accumulation and exchange of information and opinion. There will be brain storming sessions that are minuted, a first written draft to be discussed further, reviewed, amended, rephrased or thrown out altogether in favour of a fresh attempt. The whole exercise will only succeed and lead to a satisfactory outcome if there is an honest exchange of ideas and views, even the half-baked and unpopular ones. The public at large can not reasonably expect to be given access to such deliberative processes - not until a final draft is completed, which must then, of course, be open to public debate.

> Disclosure of all or part of the information may be refused if it involves the expressing of opinion, advice or recommendation by a public body, employee thereof, or any person acting on behalf of a public authority, for the purpose of assisting to formulate a policy or take a decision, if
>
> (a) it could reasonably be expected to frustrate the deliberative process by inhibiting the candid communication within or between public authorities.

In order to exclude any abuse of this provision, there should be a clear distinction made between opinions

(which are protected) and facts contained in a document (which should be accessible to the public). For this reason a second “if” should be added:

> (b) it does not contain factual, statistical, scientific, or technical information.

Severance

Following on from what has just been said on information or records being accessible only in part while the rest may be exempt from disclosure, this is a provision that the legal eagles have introduced to cover such cases in general. Public bodies should not be allowed to deny access to information in their possession just because some of it is confidential in terms of the act.

> If part of the requested information is determined to be exempt, the competent authority shall sever the part and disclose the remainder of the information.

Frivolous requests

This exemption must be handled with care, but in the interest of keeping the whole system workable, it may be a good idea to include it in the law. There may be some people who - with too much time on their hands, with a chip on their shoulder, or just for the sheer fun of making a nuisance of themselves -

will demand copious records on anything and everything. This might put the authorities' capacity to deliver under severe strain and block access for genuine requesters. In order to prevent such abuse a clause along these lines could be included:

> A request for access to information may be refused if it is manifestly frivolous or vexatious.

Obligatory disclosure in the public interest

This is a very important general rule. If one really takes seriously the right of citizens to be fully informed about the actions of public bodies on their behalf, it might appear almost like a matter of course, but it still needs to be spelt out clearly. No access to information law will be complete without a clause to this effect - known as the "public interest override" in legal terms. In plain English: No exemption, however plausible, must be used by the authorities to hide evidence of wrongdoing of officials or potential dangers. In such cases, the public interest and the public's right to know overrides any other concern or confidentiality argument. The appropriate clause could read like this:

> Notwithstanding any provisions on exemptions, access to information must be granted if
>
> (a) the disclosure of the information would reveal evidence of
>
> i. a substantial contravention of, or failure to comply with, the law, or

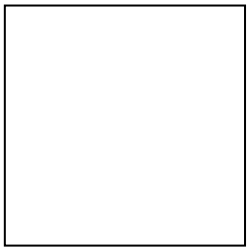
ii. the existence of any offence or miscarriage of justice, or

iii. abuse of authority or neglect in the performance of an official duty,

iv. unauthorised use of public funds, or

v. danger to the health or safety of an individual, the public or the environment; and

(b) the public interest in the disclosure of the information clearly outweighs the harm sought to be prevented by the exemption.



6. How should access to information actually work?

The clear and obvious answer is: With as little fuss as possible. If every citizen has the right to gain access to information held by public bodies, the procedure to follow must be easy even for those not used to deal with bureaucracies.

With this in mind, the best option would be to have one central port of call as suggested earlier: All requests are addressed to a commission or a commissioner who will channel them to the right public body and follow up on delivery. The greater the demand for information, however, the bigger the workload for this institution, with the result that yet another large and costly bureaucracy might develop in order to keep up with the job. Such a centralised solution, therefore, might not be practical in countries with sizeable populations. They would be better served by dedicated information officers in all the different public bodies.

Whoever the institution or person in charge, the law must stipulate that all requests are processed fairly and promptly within set time frames. A step by step approach could look as follows:

- A citizen (requester) writes to a public body and asks for a certain document, giving as many particulars as possible to allow for easy identification of the record, as well as his/her full name and all the relevant contact details. Illiterate requesters should mandate a relative, friend or neighbour to write on their behalf.

- All public bodies will be obliged by law to render any reasonable assistance, free of charge, that may be necessary to enable citizens to write a proper request.

- The clock will start ticking from the date a request is received. Most acts set deadlines for processing at between 8 and 14 days. 60 days, the period allowed in South Africa, is now regarded as far too long, especially in the case of requests from the media.

- If the request was addressed to the wrong public body, it must not simply be returned to sender or disregarded, but channeled to the correct body.

- If access to the information is granted, either in whole or in part, the public body will inform the requester in writing that

- it is available for access in the offices of the body (if it is of large volume or in a form not easily replicated), or
- can be photocopied or printed at the expense of the requester.
- Alternatively, the body will include copies or printouts of the requested information if the costs do not exceed a certain limit.

- If access to the information is denied, either in whole or in part, the body will also inform the requester in writing, including
  - the legal reasons for the refusal, and
  - advice on how to appeal against the decision.

In addressing the issue of costs, the interests of the state which can not be expected to bear unlimited expenses, will have to be balanced against those of the individual citizen who may be unable to pay the required fee. Many countries have found a middle way: no fees or taxes for requests may be levied, but public bodies may invoice requesters for photocopying/printout costs, with a certain small number of copies (e.g. the first ten pages) being free of charge.

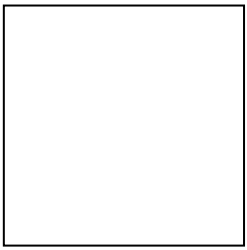
What happens if public bodies, more particularly the persons designated to deal with requests for information do not comply with all these citizen-friendly rules? If they do not deliver the goods in time or, much worse: if they pretend that files do not

exist, or tamper with or even destroy them in order to hide a possible scandal?

The drafters of the Freedom of Information Bill in Zambia have made provision for the Public Information Commission to also have the right to set a final deadline to the body in question. If it still fails to deliver, the commission can apply to the High Court to compel it to obey the law. If the judges rule accordingly, the body or responsible officer will be in contempt of court if they still refuse to act - and that is a punishable offence. Where there is no such commission in place, the Ombudsman or the Human Rights Commission could take similar action on behalf of the requester.

The much graver case of active obstruction obviously warrants harsher measures. The South African act could serve as a guideline:

> A person who with intent to deny a right of access in terms of this Act
>
> > (a) destroys, damages or alters a record;
> >
> > (b) conceals a record; or
> >
> > (c) falsifies a record or makes a false record,
>
> commits an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding two years.



7. What about whistleblowers?

So far we have dealt with information to be released by public authorities at the request of citizens. But what if a civil servant him/herself comes across records that reveal a case of corruption or abuse of public funds or, say, a serious threat to public health, safety or to the environment? Given the public's right of access to such information, what is he/she supposed to do? Pass the information on to their superior - at the risk of being reprimanded (or worse) or the information being buried again? Leak it to the media? Or isn't it their civic duty to deal openly with such information, blow the alarm and reveal it to the public?

Some countries have introduced legislation to protect such 'whistleblowers'. This is meant to shield them from sanctions imposed by those eager to keep the information under wraps - either because it reflects negatively on themselves or because they fear for the image of the organisation. The laws differ when it comes to the procedure for whistleblowers to follow. Some say they should approach a supervising body first and not just go public straight away. That, however, will only work if

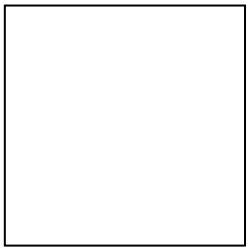
the law contains a clear obligation on those supervising bodies to deal with such information brought to their attention in a prescribed manner.

Again, where a Public Information Commission is in place as envisaged by the Zambian bill, this commission as an independent institution would be the obvious addressee for whistleblowers to direct their concerns.

Article 19 suggests that whistleblowers should have a wider range of options for making their findings known: either to a body inside the administration, or by disclosing the information to other individuals, including journalists:

> (1) No one may be subject to any legal, administrative or employment-related sanction, regardless of any breach of a legal or employment obligation, for releasing information on wrongdoing, or that which would disclose a serious threat to health, safety or the environment, as long as they acted in good faith and in the reasonable belief that the information was substantially true and disclosed evidence of wrongdoing or a serious threat to health, safety or the environment.
>
> (2) For purposes of sub-section (1), wrongdoing includes the commission of a criminal offence, failure to comply with a legal obligation, a miscarriage of justice, corruption or dishonesty, or serious maladministration regarding a public body.

South Africa went a step further and introduced a Protected Disclosures Act in 2000. This act protects employees in both the public and private sector who disclose information of unlawful or corrupt conduct by their employers or fellow employees. The purpose is to encourage honest employees to raise their concerns and report wrongdoing in the workplace without fear. The act provides for several options on how to make such protected disclosure. The first port of call is the head of the organisation. If a whistleblower fears that the boss will not be taking the concern seriously, he or she can approach public institutions like the Public Protector (Ombudsman) or the Auditor-General. Under certain conditions, the whistleblower may also go public: if neither the employer nor a regulator deals with the disclosure properly, if the whistleblower fears victimisation or a likely cover-up upon bringing the matter forward, or if the concern is “exceptionally serious”.



8. What to do about Official Secrets Acts?

Most African countries still have official secrets acts in place. In Kenya, for example, such an act effectively makes all government information off limits for the general public. All public officials are obliged to withhold information that is deemed "classified". What exactly should fall into that category is not defined and obviously left to the discretion of individual administrators. Any citizen wishing to access such information has to prove that it ought to be declassified - to the satisfaction of the official who declared it classified in the first place. Officials who release "classified" information risk being sentenced to a jail term of up to 14 years.

Another example is Botswana. The country's National Security Act 1986 follows the wording of many similar official secrets acts inherited from the colonial masters. Among others, it says that "any person who, for any purpose prejudicial to the safety or interests of Botswana … obtains, … communicates in whatever manner to any other person any secret … document, article or information that is … useful to a foreign power or disaffected person … shall be guilty of an offence and liable on conviction to a term of imprisonment

not exceeding 30 years". And the act goes further: "Any person who communicates any classified matter to any person other than a person to whom it is authorized to communicate it" could face up to 25 years in prison, even without being aware that the information was supposed to be secret. Under the act it will not be a "defence for the accused person to prove that when he communicated the matter he did not know and could not reasonably have known that it was a classified matter".

This is strong stuff, likely to make even the most ardent supporters of the public's right to know shake in their boots - and shut up. Imagine the law-abiding public servant who receives a request for information. He/she is usually under an oath of secrecy and not likely to attempt a generous interpretation of what deserves to be accessible or not. If there is only the slightest doubt whether the requested document may be classified or not, access will be refused.

Does the existence of such acts not make a mockery of any attempt to introduce access to information legislation and implement it successfully? Not necessarily. What will have to be done, though, is to apply the "three-part test" introduced in Tool Box 1 to them as a yardstick to decide whether the restrictions they place on rights and freedoms are justifiable. To pass this test, such legislation must have been enacted by parliament, not imposed by a presidential decree or in a similarly undemocratic fashion. It must protect a legitimate interest and - most importantly - be necessary in a democratic society: relevant and

sufficient reasons must be given for it and it must be proportionate to the expressed aim.

National security might be such a legitimate interest, but provisions in this regard often fail the first and even more so the third part of the test. Many existing secrecy acts - like the ones cited earlier - are so vague that it would be practically impossible for civil servants to know when issues of "national security" might not be affected and information hence not be regarded as classified. The authorities have broad discretion to declare "classified" whatever they deem fit without giving any, let alone convincing reasons. As the Court of Appeal in Tanzania found in this context, "a law must be lawful in the sense that it is not arbitrary. It should provide adequate safeguards against arbitrary decisions and provide effective control against abuse by those in authority when using the law".

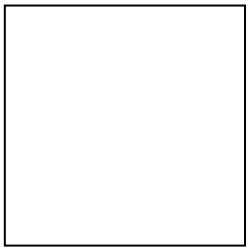
As to being "necessary" in a democratic society in the sense of being proportionate to the aim of safeguarding national security, most such laws leave much to be desired. They usually go overboard and indiscriminately block access to a wide range of information only loosely related to security concerns. An Article 19 study on "Freedom of Information in Southern Africa" published in October 2000 says:

> "The secrecy provisions in place in southern Africa fail to differentiate between legitimate and illegitimate national security interests. In practice, they prohibit communication of virtually all official information, even tangentially

> connected to security issues, even where release of the information concerned could not possibly harm a legitimate national security interest. Section 3(b) of the Botswana National Security Act, for example, forbids the dissemination of any information whatsoever which might possibly be useful to a disaffected person either directly or indirectly. This would cover, for example, information relating to corruption or mismanagement within the armed forces. The disclosure of such information would not harm national security; indeed in many cases such disclosure would promote it by helping to root out the corrupt and enhancing the efficiency of the armed forces. The range of innocuous information which might be covered by such a provision is almost infinite and its suppression cannot be regarded as a necessary and proportionate response to the need to protect national security."

Existing official secret acts should be reviewed and amended to conform with democratic principles. Where this is not immediately possible or likely to slow down or hinder the passage of access to information legislation, one could look at including an additional section in the new law. This will make provision for all "classified" information to be tested against the same standards as any other: it can only be exempted from disclosure if that is necessary, justifiable and proportionate, and – most importantly – if that is not contrary to the public interest. One could also follow the Zambian route and include a clause like the following:

“Notwithstanding any other law, no civil or criminal proceedings shall lie against a member or member of staff of the [Public Information] Commission, a public authority or a person acting on their behalf, for the disclosure of any information or for any other act done in good faith pursuant to this Act.”



9. How should the law be implemented?

Drafting the law may be comparatively easy, more so perhaps than the lobbying process to convince decision makers in government and parliament of the need for such legislation. The real test will be its implementation.

Take the South African experience, for example. There the act took effect in March 2001, but as one critic put it: “the government’s compliance with the Act is poor, sometimes bordering on the pathetic”. By 2003 only 1 % of government bodies had worked out an internal plan on how to implement the new law. According to the act, public bodies have to submit annual reports on requests for information received to the Human Rights Commission which supervises the implementation of the act. In 2003, only 15 out of 800 public bodies did so, and among the defaulters was parliament itself, the author of the act. A study published in 2004 found that nearly two thirds of all requests were simply met with silence. On the demand side, the actual number of cases where requesters made use of the act has been minimal.
Compare this with the statistics elsewhere in the world. Australia, for example, has had an access to

information act in place since 1982 and, on average, 60,000 requests are received by public bodies each year, ninety percent asking for personal information and 10 percent for policy-related documents. Appeals bodies are getting only 400 complaints a year. In Canada (Access to Information Act in force since 1983), up to 20,000 requests are processed annually. According to 2000/01 figures, information was released in full in 37.5 percent, and in part in 35 percent of these cases, nearly four percent fell under exemptions and over 20 percent were unsuccessful because there was insufficient information or records demanded did not exist.

So - is the South African law, hailed as one of the most progressive in the world, a failure? Of course not. New legislation like this, which challenges traditional perceptions and ingrained institutional habits, needs time to sink in and become part of the furniture, to be used matter-of-factly by all sides. Younger democracies, like South Africa, have not had that time yet. But there are some lessons to be learnt from the comparison.

The first is that there must be an agency in charge of continuously looking after the implementation of the law and driving the process. The Human Rights Commission in South Africa obviously does not have the capacity to do that on top of all its other responsibilities. And there was a kind of vicious circle at work: demand for information was low, so public bodies did not have to respond to a routine flow of requests and thus saw no urgent need for developing appropriate procedures. According to

research some of them had not even heard of the act by 2003.

Had there been a Public Information Commission in place, as envisaged in Zambia and indeed in Canada, the situation would certainly be different. Such a commission would start its work with a sustained public awareness campaign targeting both public institutions and the general public. If people do not know their duties or their rights - how can they be expected to respect or make use of even the best intentioned legislation?

Civil society can and must also play a role. In South Africa, an Open Democracy Advice Centre now gives legal assistance to requesters, initiates test cases and issues regular reports on progress with regard to the implementation of the act. The lessons drawn from all these experiences will be important for groups in Africa that may want to follow the example from the southern tip of the continent. Perhaps the most important lesson so far is that a good access to information law must also be clear on what sanctions can be imposed if state bodies fail to meet their obligations. Voluntary compliance may be the mark of a good citizen just as much as it is of a responsible public body. But then, both are only human and may need some gentle, or not so gentle, prodding.

And a final lesson: no democratic society should adopt an existing law or a proposed model blindly without taking into account its own specific circumstances. This goes even for the proposals made in this Tool Box.