



Open Government: A Journal on Freedom of Information

www.opengovjournal.org

Table of contents Volume 2 Issue 2

- Editorial
- Marc-Aurèle Racicot: Third Party Exemption: Discussion of the Issues and Suggestions for the Implementation of the India's Right to Information Act 2005 in Light of the Canadian Experience
- Martial Pasquier & Jean-Patrick Villeneuve: Access to information in Switzerland. From secrecy to transparency
- José Angel Martínez Usero: Evolution of freedom of information related law in Spain: new prospects for a more open government
- Marcus Turle: Confidential and commercially sensitive information – stopping public Authorities releasing information in the UK
- Graham Sutton & Sarah Holsen: China progresses information access and data protection laws
- Book review: Hood, C & Heald, D (eds) (2006) Transparency: the key to better governance?

Author: Marc-Aurèle Racicot*

Assistant Adjunct Professor and Information Access and Protection of Privacy (IAPP)
Certificate Program Manager at the University of Alberta

Title: Third Party Exemption: Discussion of the Issues and Suggestions for the Implementation of the India's Right to Information Act 2005 in Light of the Canadian Experience

Volume 2 issue 2

Abstract

In this article, the author examines the third party exemption of India's Right to Information Act, 2005. In his analysis, he identifies and discusses the principles on the need for transparency in contractual relationships between the government and private parties. The author identifies potential problems in the RTI Act, 2005, and in light of the Canadian experience with the 24 year old Access to Information Act, proposes ways to circumvent them or minimize their impact on the implementation of the Act.

Introduction

The Indian Right to Information Act, 2005 ("RTI Act") repealed and replaced a 2002 statute, the Freedom of Information Act, which was highly criticized and never came into force (Slough, 2005; Bhushan, 2002; Joshi, 2002). The two main criticisms were that it contained no provision for penalty for willful nondisclosure of information or for willfully incorrect disclosure of information by a government authority, and that there was no provision for an appeal to an independent authority (Bhushan, 2002). The Indian Government passed the RTI Act with amendments by the Lok Sabha on May 11, 2005 and the Rajya Sabha on May 12, 2005. The RTI Act has been in force since November 2005 but India adopted a very limited number of rules and some existing States' legislations were repealed.

It has been 24 years since the Canadian Access to Information Act (R.S.C. 1985, c. A-1) (ATIA) was passed but a true culture of openness has not yet been realised. For the legislation to be meaningful, FOI education cannot be limited to government officials; citizens and private organizations must also understand how the legislation works and how it may affect them when dealing with the public organizations.

Objectives

This paper specifically examines the third party exemption and notification process of the RTI Act. Proposals to circumvent potential difficulties when applying this exemption and notification process are given by comparing it with the Canadian experience. This exemption has been a major ground for litigation under Canada's ATIA. The principles involved when balancing the right of access and the need for confidentiality are discussed, as is how the RTIA third party exemption procedure can be approached in a way that promotes the purpose of the Act and not as a means of hindering disclosure.

The Process under Indian Legislation - The Right to Information Act, 2005

Pursuant to sections 5 and 6 of the RTI Act, requests for access to information from a public authority are made to a CPI Officer¹, to the State Public Information Officer, or to their Assistants. The Officer responsible for the disposal of the request must first take into consideration any representation made by a third party under section 11, with the exemption based on Parliament's consideration that individuals/organizations providing information to the Government may object to its general release. Paragraph 2(n) of the RTI Act contains a specific definition of the term:

"Third party" means a person other than the citizen making a request for information and includes a public authority.

The Act also contains a specific exemption to 'third party information' and provides for a very specific notification process for it. Exemptions from disclosure are found in section 8 of the Act, as follows:

Notwithstanding anything contained in this Act, there shall be no obligation to give any citizen,— [...]

Information including commercial confidence, trade secrets or intellectual property, the disclosure of which would harm the competitive position of a third party, unless the competent authority is satisfied that larger public interest warrants the disclosure of such information; [underlining added]

¹ Pursuant to subsection 1(2), the Act "extends to the whole of India except the State of Jammu and Kashmir." Hence, the RTI Act applies to the Central Government as well as to the State's Governments. For the purpose of this paper, I will only refer to the Central Government regime (ex. Central Public Information Officer), unless otherwise mentioned.

Use of the term 'including', makes it clear that the information is not limited to commercial confidence, trade secrets or intellectual property. Another relevant exemption deals with 'personal information'. Unless large public interest justifies it, there is no obligation to disclose information which has "no relationship to any public activity or interest" or if it "would cause unwarranted invasion of the privacy of the individual."

The application of these discretionary exemptions requires a two-step process. The CPI Officer must make a finding of harm; then, further to finding potential harm, s/he must determine whether the record should nevertheless be disclosed in the public interest. Finally s/he must consider the exceptions/overrides to these exemptions as discussed below.

The RTI Act provides for greater flexibility in disclosure. The opening wording of section 8 "...there shall be no obligation to give..." is interesting. In the Canadian legislation the words "...shall refuse to disclose..." are used. In the former wording it is understood that although there is no obligation to give, there is discretion to do so.

The language used in section 8 – "there shall be no obligation to give any citizen" - and the language of RTI subsections 8(2) and (3), clarifies the intent of the legislator to maximize disclosure of information in the public interest by establishing criteria to assist the CPI Officer's decision. 8(2) provides a general public interest overriding clause and an additional 'public interest override' is found in subsection 11(1) in fine. 8(3) provides a 20-year overriding clause which applies to various references to 'third party information' and 'personal information'.

If a case of 'third party information' meets the injury test and does not qualify in the listed exceptions or overriding clauses, the CPI Officer is under no obligation (may refuse to disclose) to give information if s/he believes the disclosure will harm the competitive position of the third party and if s/he is satisfied there is no public interest in disclosing the information.

The Notification Process

The notification provision is found in section 11 of the RTI Act. Timelines are very short; typically, a response must be provided within 30 days of receipt. If the life or liberty of a person is at stake, subsection 7(1) in fine provides that " ... the information sought ... shall be provided within forty-eight hours of the receipt of the request."

Requests involving disclosure of third party information, which relates to or has been supplied by a third party and has been treated as confidential by that third party, require the Officer to give written notice to such third party and invite him/her to make an oral or written

submission within five days from the receipt of the request. Hence, the three prerequisites for the notification process are:

- (1) the CPI Officer must intend to disclose the information;
- (2) the information must relate or must have been supplied by a third party; and
- (3) the information must have been treated as confidential by the third party.

The third party has 10 days from receipt of the notice to make his submission.

Notwithstanding the 30 days mandated by section 7², the CPI Officer must, within 40 days after the receipt of the request, decide whether to disclose the information and provide a written statement of his decision to the third party. An appeal under section 19 may be filed against the decision³ within 30 days. As it is not specified, it is assumed that the notice will mention that if no appeal is filed within 30 days, the requested information will be released.

The Appeal

If the third party is not satisfied with the decision made under subsection 11(3) s/he may file an appeal before the Central Information Commission within 30 days from the date of the order⁴. Interestingly, the appeal mechanism from a decision made under section 11 is found in subsection 19(2), however, the present drafting makes it questionable if a third party appeal is also available under subsection 19(1) as a 'person who is aggrieved by a decision'. Additionally, subsection 19(3) provides for a second appeal against the decision made under subsection 19(1). Note that there is no mention of subsection 19(2).

It is therefore arguable that a second appeal is not available to a third party. If subsection 19(1) was all inclusive subsection 19(2) would not exist. This indicates that the only appeal available to a third party is under subsection 19(2). Second, subsection 19(3) mentions only 19(1), whereas subsection 19(6) specifically refers to an appeal made under 19(1) or 19(2). Third, when an appeal relates to third party information, subsection 19(4) extends an opportunity for the third party to be heard. Though unusual, this limited right to appeal is consistent with the purpose of the legislation: providing citizens a meaningful right of access while still providing for exemptions. The absence of a second appeal for third parties shows that Parliament chose to put an emphasis on openness.

² Unfortunately, due to the 'notwithstanding' found in ss. 11(3), the 48 hours limit provided by 7(1) in situation where the life or liberty of a person is at stake, is pushed aside.

³ RTI Act, s. 11(4). Since there is no provision regarding time extension in the current RTI Act, a decision must be taken within the 40-day time limit found in s. 11(4).

⁴ RTI Act, s. 11(2). In Canada, if the head of the government institution is not satisfied with the third party representations and decides to disclose the information, the third party's only option to prevent disclosure is to file an application for judicial review pursuant to section 44 of the ATIA within 20 days of having been notified of the head's decision.

As of July 2006, the Central Government of India has not adopted any rules with regard to the third party exemption or notification, but has adopted some which deal with appeals to the Central Information Commission (Central Information Commission (Appeal Procedure) Rules, 2005).

The Principles

The major principles of transparency in the conduct of public administration and in contractual relations between the government and third parties merit examination.

A. Why is Transparency Paramount?

The goal of transparency in public administration is to prevent any clandestine arrangements whereby government officials and private firms collaborate to keep information secret (McMahon, 2006). The recent Canadian Sponsorship Scandal is an excellent example of the potential malfeasance transparency can prevent. The Scandal arose from the federal government's program to promote Canada at cultural or sporting events in Quebec. The program began 1996 but when it was disclosed in 2004 as corrupt, a Commission of Inquiry led by Justice John Gomery was established. In his first report released in 2005, Justice Gomery wrote:

The Commission of inquiry found: [...] a veil of secrecy surrounding the administration of the Sponsorship Program and an absence of transparency in the contracting process; [...] (Government of Canada, 2005a, p5)

There was an atmosphere of secrecy and only the inner circle was informed of decisions (p23).

In his second report of February 2006, Justice Gomery insisted on the need for transparency, noting that "An appropriate access to information regime is a key part of the transparency that is an essential element of modern public administration." (Government of Canada, 2005b, p179) He even cited the private sector as being more transparent than the public sector:

The Commission wishes to emphasize a key concept that may be learned from the private sector: greater transparency promotes accountability and better management. The best managers are those whose administrative practices are transparent and who

accept that they are accountable not only to their superiors but also to the shareholders of the corporation (p178).

Coincidentally, about the same time as the Sponsorship Program was created, John C. Pearson offered the following opinion:

While it is true all legitimate government business is conducted on behalf of the public, it does not follow all government business is best conducted in public. Indeed, the public interest is best served by government following commercial practices established by the marketplace. Commercial confidences customarily observed should be respected (Pearson, 1994, p275).

In light of the serious consequences of the Sponsorship Scandal, Mr. Pearson's opinion deserves comment. Commercial confidences customarily observed amongst private organizations cannot generally apply and do not guarantee the public interest when one of the parties is a public authority. Government officials should inform potential business associates that confidentiality will not attach to the transaction. Contracting third parties must understand that the State acts as a fiduciary on behalf of its citizens and the citizens have a right to know what the contract's terms are. Government business conducted on behalf of the public must be conducted in public. As Justice Kelen writes in *Canada Post Corp. v. Canada* (National Capital Commission):

The intention of Parliament in exempting financial and commercial information from disclosure applied to confidential information submitted to the government, not negotiated amounts for goods or services. Otherwise, every contract amount with the government would be exempt from disclosure, and the public would have no access to this important information (*Canada Post Corp. v. Canada*, 2002).

Government transparency and access to information allows citizens to supervise government activity and hold government accountable. It is critical to a properly-governed procurement policy. In *High-Rise Inc. v. Canada* (Minister of Public Works & Government Services) the Federal Court of Appeal of Canada held that maintaining confidentiality during the bidding process prevents bidder collusion and ensures competitive pricing. However, relying on *Gamma* (1994, para 8)⁵, the Court of Appeal stated that different considerations arise when

⁵ "One must keep in mind that these Proposals are put together for the purpose of obtaining a government contract, with payment to come from public funds. While there may be much to be said for proposals or tenders being treated confidential until a contract is granted, once the contract is either granted or withheld there would not, except in special cases, appear to be a need for keeping tenders secret. In other words, when a would-be contractor sets out to win a government contract he should not expect that the terms upon which he is prepared to contract,

the contract is awarded and public funds are committed. No public benefit was fostered by maintaining the confidentiality of amounts paid or payable by government pursuant to contractual obligations with third parties. In short, the Court of Appeal stated that transparency is a way of holding government accountable.

B. Contractual relations between the government and private parties

This is the third party exemption question: should contractual information between the government and private parties be subject to public scrutiny? Discussion will be limited only to contractual relations entered into by third parties of their own free will⁶.

Due to the particular wording of the Canadian exemption, some contractual information is not always "supplied to a government institution by a third party". The courts have found that negotiated rates (Halifax Development Ltd. v. Canada, 1995) or terms of negotiated contracts (Canadian Pacific Hotels Corp. v. Canada (Attorney General), 2004) are not information supplied by a third party but negotiated terms or amounts, thereby closing the possibility of raising paragraph 20(1)(b) of the ATIA as a ground of refusal. The RTI has similar wording but also provides that information relating to a third party is subject to the exemption, meaning all information – including that generated by the State related to a third party – is subject to the third party exemption. In Canada, paragraphs 20(1)(c) and 20(1)(d) cover information supplied by a third party, but for these exemptions to apply, probable prejudice must be demonstrated. The scope of the Indian exemption is similar to its Canadian counterpart.

including the capacities his firm brings to the task, are to be kept fully insulated from the disclosure obligations of the Government of Canada as part of its accountability.”

⁶ Note that section 20 exemption covers information provided by a third party to a government institution.

Discussion of the Issues and Suggestions for the Implementation of the RTI Act in light of the Canadian Experience

Examining the following issues, which in the last 20 years have proved to be potential traps or dead-end solutions in Canada, may give India a head-start in the implementation and application of the RTI Act. Suggestions to help third parties and public authorities work with the RTI Act will also be made

A. Who counts as a third party?

While similar to Canadian legislation, Indian legislation includes 'public authorities' in its definition of third party, which could make a big difference. In subsection 3(1) of the ATIA 'third party' expressly excludes any government institutions⁷.

In India, Parliament disregarded the Parliamentary Standing Committee's recommendation and adopted the Government's Bill which includes public authorities in the definition of third party. If the intention was the 'optimum use of limited fiscal resources', Parliament may have missed the bulls-eye. Since the processing public authority must notify any third party to which the information relates, it is easy to imagine a report prepared for one department, in which 10 other departments are expressly referred, resulting in a burdensome and time-consuming procedure. In light of subsection 6(3) of the RTI⁸ this notification process appears to be a waste of time, since pursuant to subsection 6(3) a request will be transferred if another public authority has more interest in it. A similar disposition is found in the Canadian legislation. Section 8 of the ATIA allows a government institution to transfer the request if "the head of the institution considers that another government institution has a greater interest in the record."

The Canadian experience is that Crown Corporations - such as Canada Post Corporation (CPC) - which are not listed in Schedule I and therefore not considered third parties under the ATIA - are free to actively prevent disclosure of their information. This has resulted in many CPC

⁷ ATIA, ss. 3(1): "in respect of a request for access to a record under this Act, means any person, group of persons or organization other than the person that made the request or a government institution." with Government Institution' defined as "any department or ministry of state of the Government of Canada listed in Schedule I or any body or office listed in Schedule I [of the ATIA]."

⁸ RTI Act, ss. 6(3): Where an application is made to a public authority requesting for an information,—

(i) which is held by another public authority; or
 (ii) the subject matter of which is more closely connected with the functions of another public authority, the public authority, to which such application is made, shall transfer the application or such part of it as may be appropriate to that other public authority and inform the applicant immediately about such transfer:

Provided that the transfer of an application pursuant to this sub-section shall be made as soon as practicable but in no case later than five days from the date of receipt of the application.

review applications being filed in Federal Court; imagine the chaos if all government institutions were considered third parties. If the goal of access to information is to facilitate access; any procedure used to delay access must be carefully analyzed.

What, then, can be done in India to ensure the system does not become congested with relentless notices to other public authorities? Clearly, any options chosen must be clearly state that the notification process must not become a way to delay access.

An obvious option is to modify the definition of third party to exclude other public authorities, using section 30 of the RTI Act. Subsection 30(1) provides that:

If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as appear to be necessary or expedient for removal of the difficulty.

Since subsection 6(3) of the RTI Act mandates that the request be transferred if the subject matter is more closely connected with the functions of another public authority, it must be assumed that the authority processing the request is the one most concerned with the information sought. Therefore it has the power to decide if the information should be disclosed without the need for representations from other public authorities.

Rules could be adopted to control the notification process. Presently, the public authority processing the request has only 40 days to locate the records, expedite the notification process (which must be initiated within 5 days from receipt) and issue its decision. This time frame makes it difficult, if not impossible, to meet the obligations of the RTI Act. The process could be facilitated by authorizing the CPI Officer to notify verbally any third parties that are public authorities.

B. What information counts as third party and what are the impacts on the Notification Process?

1. Should personal information be included?

To properly apply the notification process, the CPI Officer must understand what is meant by "third party information". Is "personal information" third party information? If the name of an individual appears in a document, can it be said that this information relates to him/her? From section 11 of the RTI Act, it is not clear if the notification process will apply to the release of personal information.

At the Canadian federal level, the third party notification process (found in sections 27, 28 and 29) only deals with commercial information or information that could be harmful if disclosed. It allows a third party to make representation regarding the nature of the information and the magnitude of injury it may suffer resulting from the disclosure, and, if the disclosure is based on section 20(6) of the ATIA, to demonstrate that such injury outweighs the public interest. A third party will be notified only if the head of a government institution intends to disclose the information in response to a request (section 27) or if the head of a government institution intends to disclose on the recommendation of the Information Commissioner as a result of a complaint (paragraph 29(1)(b)).

In Canada, an interesting distinction between the federal and many provincial statutes is that the federal notification process deals only with commercial information: an individual whose information does not fall within section 20 of the ATIA will not receive notice if the head of a government institution intends to release that information. Canada also has privacy legislation with which the government must comply; there is no privacy legislation applicable to public authorities in India. Some Canadian provinces have included individuals in the definition of third party, and in the case of the potential release of personal information, have mandated a notice to the individual concerned (Alberta Freedom of Information and Protection of Privacy Act, 2000)

Based on interpretation of the RTI Act, a third party whose personal information is to be disclosed should also receive a notice for the following reasons:

- a. third party is any person other than the requester;
- b. there shall be no obligation to give any citizen information which relates to personal information; and,
- c. notification is required when the CPI Officer intends to disclose information which relates or has been supplied by a third party.

As there is no suggestion that the notification process is limited to commercial third parties, it appears that a notice will be sent to anyone whose personal information is to be disclosed to an access requester. Since there is no privacy legislation in India, this notification is critical, since this it would be the only protection afforded an individual before disclosure, allowing the third party to justify the non-disclosure and to balance the public interest in disclosure.

2. The Indian Legislation contemplate broader notification

There is a subtle but very important difference between the Canadian and Indian notification processes. Use of the words "relating to" in subsection 11(1) of the RTI extends the

notification process further than is provided in Canada, perhaps because the Canadian process does not extend to personal information, as does the Indian Act.

The minimal requirement for notification in the Indian Statute regarding information 'which relates to a third party' seems to indicate that 'personal information' is subject to notification, providing greater protection to all third parties. In Canada, notice to a third party will be sent only if the head of the government institution intends to disclose information that falls in section 20, whereas in the RTI Act it seems sufficient for the name of a third party to appear in a document for a notice to be required. This may make it more difficult for the CPI Officer to notify all the individuals and organizations concerned within the time limits. It could be argued that the Indian notification is broad because it is required if the information 'relates to' a third party. Conversely, it may also be construed as being very narrow because the notice is required only if the information 'has been treated as confidential by the third party'.

Difficulties in the determination of the first requirement (that the information relates to or has been supplied by a third party) are not anticipated because (1) the language used to define 'third party' is broad and vague, and based on experience, (2) Canadian courts have given a broad interpretation to the term 'third party' (*Canada Post Corp. v. Canada (Minister of Public Works)*, 1993; *Rubin v. Canada (Minister of Health)*, 2003). However, the second requirement (that the information has been treated as confidential by the third party) raises the question of how the CPI Officer will determine the 'information has been treated as confidential by the third party' without the benefit of the third party's representations? In Canada, notification is usually sent to obtain representations which will help determine if the information has been treated confidentially⁹. To minimize the impact these provisions might have on the communication of information it is suggested that the term 'which relates to' found in subsection 11(1) of the RTI Act be explained or defined in the Rules.

C. Who decides?

Maja Daruwala, CHRI Director (Letter from Maja Daruwala, 2005) has raised the issue that three authorities have been given concurrent powers to determine what can be disclosed in

⁹ Reception of the request initiates the process. The government institution has 30 days to give a response to the requester. Once the records have been collected, that information has been identified as being potential s. 20 information and that the head intends to disclose the records, a notice will be sent to the third party, if he can be reasonably located (s. 27). The third party will have 20 days to make his representations (s. 28). It is possible for the head of the government institution to extend the 30-day time limit to respond to the request, if the consultations with the third party go beyond the limit. The extension of time must be notified before the 30-day time limit is over. (See para. 9(1)(c) of the ATIA) Upon reception of the representations, if the head still intends to disclose the requested records, he will give notice to the third party that the records will be disclosed to the requester unless the third party brings, within 20 days, an application for judicial review under section 44 of the Act.

the public interest¹⁰. Sections 8(1)(d), 8(2), 8(3) and 11(1) of the RTI Act all contain a public interest override clause. This raises two questions: who will make the determination and what will be the criteria for their application?

1. Who will make the determination?

The trio of decision makers seems an obvious practical error, which could be amended forthwith pursuant to section 30 of the RTI Act by removing competent authority from all decisions. These should ultimately reside with the Public Information Officer, as seems the intent pursuant to sections 5, 6, 7 and 11. While paragraph 8(d) mentions the competent authority, subsection 11(1) mentions the CPI Officer; clearly this is a legislative oversight. With regard to the third party exemption, subsections 7(7) and 11(3) leave little doubt that the decision rests with the CPI Officer.

2. What will the criteria be?

In a research paper prepared for the Canadian Access to Information Review Task Force, Barbara McIsaac notes that due to a lack of direction and guidance in the application of discretionary exemptions the perception is "that when there is any doubt about what to do the doubt is resolved in favour of invoking the exemption." (McIsaac, 2001). The Task Force concluded that "The exercise of discretion inherently implies a consideration of the factors relevant in each particular case, including any anticipated harm from disclosure." (Government of Canada, 2002, 43) It added that "in exercising discretion, institutions should consider the fact that information usually becomes less sensitive over time" (p43-44) and that "The application of exemptions should not be a matter of intricate legal reasoning, but of basic questions asked consistently at all stages in the process: Are there good reasons for withholding the information in this case? How soon can it be made available without causing harm to one of the interests protected by the Act?" (p43-44).

The Government should identify criteria to assist CPI Officers when making their decisions, including such factors as:

¹⁰ "Section 8(2) of the RTI Act provides for a public interest override even where information requested is covered by one or more of the exemptions in s 8(1). Section 8(2) explicitly provides that the decision making power as to what is in the public interests vest with the "public authority". [...]

However in three categories of exempt information listed in Sec. 8(1) [8(1)(d), (e) and (j)], three more entities namely, the competent authority, the Public Information Officer and the appellate authority have been given specific powers to determine whether information needs to be disclosed in public interest. [...] PIOs and Appellate Authorities will need clarification as to how Sec. 8(2) will be reconciled with Sec. 8(1)(d), (e) and (j) as different entities have been provided concurrent jurisdiction on the same subject. It is also necessary to clarify whether the release of information can be secured upon the order of the Departmental Appellate Authority or the appropriate Information Commissioner based on the merits of the case or this has to wait until the competent authority concurs with their decision. Furthermore it needs to be clarified whether the PIO has the power to communicate with the appropriate competent authority seeking permission for release of the information rather than issue a rejection order outright. If yes will the deadline of 30 days continue to apply to this case considering the usual delays that may occur while in taking decisions on such controversial matters."

- a. the general purpose of the legislation;
- b. the wording of the discretionary exemption and the interests which the exemption attempts to protect;
- c. the nature of information;
- d. the commercial context;
- e. the potential uses/misuses of information;
- f. the “subjective”, contractual, expectation of confidentiality;
- g. the reasons for promoting non-disclosure of information?
- h. the whether the requester’s request could be satisfied by severing the record (s. 10 of the RTI Act) and by providing the requester with as much information as reasonably practicable;
- i. the historical practice of the institution respecting the release of similar types of records (the RTI Act is not intended to limit disclosure of information that was available to the public before it came into force);
- j. the age of the record;
- k. the public interest in disclosing the record.

In Canada, exceptions to the third party exemption can also be found in subsection 20(2), (3) and (4) [environmental testing]; 20(5) [consent for disclosure]; and, 20(6) [public interest override]. The latter exemption has rarely, if ever, been utilized and is not easy to apply since it bestows the discretion on heads of government institutions to disclose third party information, which otherwise must be exempt, on a mandatory basis by invoking a public interest “override” (Treasury Board of Canada, 2002). In another research report prepared for the Access to Information Review Task Force, Rankin and Chapman write that “experience shows that the public interest override has been applied sparingly, even in jurisdictions like British Columbia, where the override provision is broad and applies to all exemptions.” (Rankin & Chapman, 2001) The Task Force opined that a general public interest override is unnecessary because “[D]iscretionary exemptions already imply a balancing of the public interest in protecting the information, and the public interest in disclosure, and the mandatory exemptions, for third party and personal information already include specific overrides.” (Government of Canada, 2002, p43).

D. What are the procedural time limits?

It seems that this issue is really just another oversight, or legislative ‘typo’. As previously identified, the time limits are very short and some provisions lack clarity. First reading of the Act seems to indicate a notification will be required each time a CPI Officer intends to disclose

information (including personal information)¹¹ or records which relates to or has been supplied by a third party. While it is reasonable to require notice where a third party's personal information is involved, it is very difficult to imagine how the CPI Officer will locate the documents, identify and notify any third parties, and determine if the information has been treated confidentially by the third party, within five days of the receipt of the request. Hence the need for guidelines. A possible solution could have the Rules state that to be considered to 'have been treated in a confidential manner', a third party that provides information to a public authority must notify the public authority at the initial time of communication, that the information is treated as confidential and that without such notice, the information will not be treated as confidential. The rules could also provide that if the information is personal, or is a trade secret, it should be deemed information treated in a confidential manner by the third party.

1. When can a requester file a complaint?

Under section 7, a response must be given to the requester within 30 days of receipt of the request, but section 11 provides that, if a third party is notified, a decision must be made within 40 days. How, then, will a requester be aware of the third party consultation if s/he receives no notice? A notice for time extension could be sent, or made via telephone, to the requester indicating that the process may now take up to 40 days. If a decision is not received within that time, an appeal may be filed.

2. How much time should an appeal take?

In its current version the RTI Act subsection 19(6) refers to 19(1) and 19(2). There is reference to a 30-day time limit to dispose of the first appeal found in subsection 19(1) but no limit for the second appeal found in subsection 19(3). This may be an oversight: subsection 19(6) should have referred to subsection 19(1) and 19(3). This oversight could be amended as follows, 19(6) should read:

"An appeal under sub-section (1) or sub-section (2), or a second appeal under sub-section (3), shall be disposed within thirty days of the receipt of the appeal, or second appeal, or..."

Conclusion

With the RTI Act, India took a big step towards acquiring more transparency and accountability from its government, but this step does not guarantee any inherent 'culture of

¹¹ The definition of "information" at paragraph 2(f) is very wide.

secrecy' has or will disappear. The Act is not without imperfections, nor without remedies. A culture of openness must be nurtured and encouraged by ministers and management. Awareness of the issues and the development of rules, policies and guidelines are most important and in this vein, the following advice to 'commercial' third parties and to public authorities is offered.

Third parties should clearly mark commercially sensitive documents, including current contact information, to help the CPI Officer processing a request, thereby ensuring that notification will be sent. A third party should attach a covering letter to the CPI Officer, mentioning that the documents contain section 8(1)(d) information and that if the CPI Officer intends to disclose such information a notice is required (Drapau & Racicot, 2005, pp5-84). Finally, the person who will be responsible for receiving and responding to the notice must be identified, as the time allotted for the response is only 10 days. When responding to a notice, third parties should make written representations, which evidence may prove useful during the 'review/appeal' process. Some specific initiatives proposed by Colin McNairn and Christopher are:

- 1) Following information management procedures that evidence a consistent practice of treating the particular kind of information as confidential;
- 2) Asserting confidentiality for the information when submitting it to a government institution;
- 3) At the same stage, noting the potential for harm, should the information be disclosed. (McNairn & Woodbury, 1992, pp4-15)

Third parties should be informed that any information provided by them is subject to the RTI Act and may 'potentially' be released if an access request is made. Public authorities should prepare frequently asked questions (FAQ's) for the third party. As previously mentioned, it is paramount that administrators in every level of government remember that public and private education is the key to lasting success in implementing FOI legislation.

References

*Marc-Aurèle Racicot is Assistant Adjunct Professor and Information Access and Protection of Privacy (IAPP) Certificate Program Manager at the University of Alberta. He would like to thank Professor Wayne Renke for his guidance and all my friends at Commonwealth Human Rights Initiative (CHRI) for their invaluable comments on earlier versions of this paper.

Access to Information Act (R.S.C. 1985, c. A-1)

(Alberta) Freedom of Information and Protection of Privacy Act, R.S.A. 2000, c. F-25 as amended, para. 30(1)(b); (Ontario) Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F-31 as amended, section 28.

Bhushan, P (2002) India Approves Freedom of Information Law: The Freedom of Information Bill 2002, National Campaign Committee for the People's Right to Information, December 2002. Available at: www.freedominfo.org/news/india/

Central Information Commission (Appeal Procedure) Rules, 2005 [dated October 28th, 2005: to be published in the Gazette of India, Part II, section 3, subsection (i)] Available online at: www.righttoinformation.gov.in

Canadian Pacific Hotels Corp. v. Canada (Attorney General), 2004 FC 444 at paras. 36-37, in Drapeau and Racicot, p. 1-311; Canada Post Corp. v. Canada (National Capital Commission), 2002 FCT 700 at para. 14, Drapeau and Racicot, p. 1-311.

Canada Post Corp. v. Canada (National Capital Commission), 2002 FCT 700 at para. 14; M.W. Drapeau and M.-A. Racicot, Federal Access to Information and Privacy Legislation Annotated 2006, (Toronto: Thomson-Carswell, 2005), p. 1-311.

Canada Post Corp. v. Canada (Minister of Public Works), [1993] 3 F.C. 320 at 328, in which the court found that CPC was a third party because it was neither the person that made the request nor a government institution.

Daruwala, M (2005) Letter from the Director, Commonwealth Human Rights Initiative, addressed to Shri A N Tiwari, Secretary for Personnel, Ministry of Personnel, Shri T K Vishwanathan, Secretary for Legislation, Legislative Department, Ministry of Law and Justice, Shri T Jacob, Joint Secretary, Department of Personnel and Training. New Delhi, August 9, 2005.

Drapeau, M and Racicot, M (2005) Federal Access to Information and Privacy Legislation Annotated 2006. Toronto. Thomson-Carswell, pp. 5-84.

Freedom of Information Act, 2002, No. 5 of 2003, The Gazette of India, Registered No. DL-33004/2003.

Government of Canada (2005a) Commission of Inquiry into the Sponsorship Program and Advertising Activities, Who is Responsible? Summary, Report 1, November 2005, p. 5 Available online at: www.gomery.ca/en/phase1report/summary/es_full_v01.pdf

Government of Canada (2005b) Commission of Inquiry into the Sponsorship Program and Advertising Activities, Restoring Accountability – Recommendations, Report 2, February 2006, p. 179 Available online at: www.gomery.ca/en/phase2report/recommendations/CISPAAR_Report_Chapter10.pdf

Government of Canada (2002) Access to Information Review Task Force, Access to Information: Making it Work for Canadians, Report, June 2002 at p. 43 Available online at: www.atirtf-geai.gc.ca

Halifax Development Ltd. v. Canada (Minister of Public Works & Government Services), [1994] F.C.J. No. 2035 (QL)(Fed. T.D.), in Drapeau and Racicot, p. 1-301; Perez Bramalea Ltd. v. Canada (National Capital Commission), [1995] F.C.J. No. 63 (QL)(Fed.T.D.), in Drapeau and Racicot, p. 1-307.

High-Rise Inc. v. Canada (Minister of Public Works & Government Services) (2004) FCA 99 at paras. 40-43.

Joshi, A, Freedom of Information in India, paper presented in Conference on Freedom of Information and Civil Society in Asia, April 2001. Available at: www.foi-asia.org/India/Confreport_India.html

Barbara McIsaac (2001) The Nature and Structure of Exempting Provisions and the Use of the Concept of a Public Interest Override, Report 17, Access to Information Review Task Force, Available online at: www.atirtf-geai.gc.ca/paper-nature1-e.html

McMahon, K (2006) Procurement issues go primetime: Public institutions need to build public confidence, Law Times, Vol. 17, No. 4, January 30, 2006, p.1.

McNairn, C and. Woodbury, C (1992) Government Information: Access and Privacy, (Toronto: Thomson-Carswell), pp. 4-15.

Pearson, J (1994) Access to Confidential Business Information in Government Files, in Yves-Marie Morissette, Wade MacLauchlan and Monique Ouellette, Open Justice / La transparence dans le système judiciaire, Canadian Institute for the Administration of Justice, (Montréal : Les Éditions Thémis, 1994) p. 275.

Rankin, M & Chapman, K (2001) Third Party Provisions, Research Report 19. Available online at: www.atirtf-geai.gc.ca/paper-thirdparty1-e.html

Right To Information Act, 2005, No. 22 of 2005, The Gazette of India, Registered N. DL-(N)04/0007/2003-05 (hereinafter the "RTI Act"), section 31.

Rubin v. Canada (Minister of Health), 2003 FCA 37 at paras. 8-9, in which the court of appeal found that nothing in the ATIA indicate that a foreign government cannot be a third party.

Slough, P and Rodrigues, C (2005) India's Right to Information Movement Makes A Breakthrough. Open Government: a journal on Freedom of Information. Volume 1 Issue 1 Published 21 March 2005 at p. 3. Available at www.opengovjournal.org

Société Gamma Inc. v. Canada (Department of Secretary of State), [1994] F.C.J. No. 589 (QL) (Fed.T.D.) at para. 8

Treasury Board of Canada (2002) Access to Information: Policies and Guidelines, Chapter 2-8 Available online at: www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_121/siglist_e.asp

Authors

Dr. Martial Pasquier, Professor
Public Management and Public Marketing Unit
Swiss Graduate School of Public Administration IDHEAP
Route de la Maladière 21
1022 Chavannes-près-Renens
Switzerland
martial.pasquier@idheap.unil.ch

Jean-Patrick Villeneuve
Research and teaching assistant
Public Management and Public Marketing Unit
Swiss Graduate School of Public Administration IDHEAP
Route de la Maladière 21
1022 Chavannes-près-Renens
Switzerland
jean-patrick.villeneuve@idheap.unil.ch

Title: Access to information in Switzerland. From secrecy to transparency

Volume 2 issue 2

Abstract

Access to information legislations are now present in over 50 countries world-wide. Lagging behind some of its own Cantons, the Swiss Federal government was until recently one of the few hold outs in Europe. But, in December 2004, the Confederation voted the 'Loi sur la Transparence de l'administration' or Law on Transparency (LTrans) a Law that came into effect in July 2006. This paper presents an overview of the new Law and underlines the main institutional challenges to its introduction in Switzerland.

Introduction

At first, linking the concept of transparency with Switzerland might seem a bit odd. In fact, to outside observers, Switzerland represents the exact opposite of transparency. With its banks, arcane federal structure and landscape of isolated mountain villages, it gives out an image of privacy and secrecy at all costs. Quite tellingly, it remains one of the few countries in Europe without a proper Law on access to information (Banisar, 2004; Mendel, 2003b). While States as different in their administrative cultures and institutional structures as Yemen, Ukraine and France have all enacted laws on access to information, how can a country such as Switzerland

do without what has come to be seen as one of the corner stones of good administrative practices ? (OECD, 2002)

There are a number of elements explaining the relative 'lateness' of the adoption of such a Law at the federal level in Switzerland. First of all, the culture of secrecy is strongly present in the Swiss administrative and social system as a whole (Kriesi, 1998). This situation should never be underestimated, and its cultural impact downplayed. Secondly, Switzerland, with its federal system, is a country where an important part of the overall policy jurisdiction lies with the Cantons and the communal entities (Kissling-Näf and Wälti, 2004). In such a context, a large amount of information directly pertaining to the citizens is held, not by the federal government, but at the smaller and more accessible Cantonal and local levels. Finally, the Swiss political system in itself also accounts for this situation. At the federal level and in most Cantons, political parties govern according to the principle of 'concordance' (Kriesi, 1998). This means that every political party, from right and left, takes part in the forming of the executive and as such has direct access to all the information produced by the administration. It also means that the political need for transparency is that much lower.

For a number of years some of the Swiss Cantons have enacted laws giving citizens access to the documents and information collected and compiled by their governments (Conseil fédéral, 2003). But, at the federal level, the challenges appeared somehow more significant. Since December 2004, this 'deficiency' has been remedied at the Federal level with the signing of the 'Loi sur la transparence de l'administration' or Law on Transparency (LTrans). The law has taken effect in July 2006.

The challenges posed by transparency laws in countries more readily 'adapted' to its realities are great, and have been documented by numerous scholars (Blanton et al., 2003; Caddy, 2001; Frankel, 2001; Hasan, 2005; Héritier, 2003; Mendel, 2003a; Roberts, 2002b; Sanchez, 2002). In Switzerland, given its institutional structure, decision making apparatus and federal construction, these challenges seem more formidable yet. This paper will briefly outline the major steps undertaken to put this bill in front of Parliament, and detail its major aspects, exceptions and caveats. As well, we shall look at some of the 'Swiss specific' challenges in implementing a law on transparency.

Switzerland and transparency: A short history

To trace back the emergence of the LTrans in Switzerland, one needs to understand the various aspects of the Swiss federal structure. The authority for numerous policies such as education, health, police, taxation, are Cantonal jurisdiction. Thus, the daily decisions influencing the lives of the citizenry are generally taken at the Cantonal level. It is also at that

level that a number of democratic advances are being made, to be later adopted at the federal level. It is perhaps in part for this reason that pressures for greater transparency were first felt in the Cantons.

The Canton of Bern, in 1993 (LIn, 1993), first introduced an Access to information law in Switzerland. Following a scandal on the existence of slush funds used to finance political propaganda, the Cantonal authorities tried to reinstitute a modicum of confidence in the administration by introducing a law on information; a number of other jurisdictions have since then followed suit: Geneva (LIPAD, 2001), Vaud (LInfo, 2002), Jura (Loi sur l'information, 2002), etc. The majority of Cantons are right now devising plans to introduce such legislation.

The signing of the LTrans in 2004 represents a major step for the Swiss federal administration. It is a step that was long in the making. The question had come to the fore at many times since the 1980s. We can find in 1982 a Commission of experts pleading for a federal project on the introduction of the principle of transparency in the activities of the administration. Similar proposals were put forward by various groups in 1986, 1989 and 1991 (Conseil fédéral, 2003).

In 1992, the Federal Council adopted in its legislative agenda the specific objective of being 'closer to citizen via increased transparency'; it wanted to examine the possibility of introducing the principle of transparency in the activities of the administration in the more general framework of governmental reform (Conseil fédéral, 2003). It is to be noted that similar steps forward, in putting transparency on the table as a subject of debate, were made through the 1990s. In April 2000, the Federal Council decided to send for consultation a bill on transparency in the federal administration. The project presented the main concept of a legislation on information and, most notably, the basic principles as to the rights of access for citizens. The general reaction to the draft project was rather positive. The criticisms levelled were nevertheless often serious, but also quite divergent depending on the group making the representations (Conseil fédéral, 2003: 1825).

Opposition was clearest from private sector enterprises and organisms regulated by special laws and belonging in part or in total to the Confederation. Representatives of the media were worried that access procedures would in fact complicate access to information (forms to fill, tighter screening of documents released, etc) that was until then obtained informally. Representatives of the economy were particularly interested in the protection of private interests (overriding private interest, business and professional secrets, patents, etc). They worried that these particular considerations might not be fully accounted for in the decisions to make public or not certain documents. Others, were worried about the overall cost of

transparency (Conseil fédéral, 2003: 1824-1825). There were a number of adaptations made to the draft project, but in essence it remained largely unchanged.

Institutional challenges

Aside from the usual reticence of public organisations to open to all their various procedures and information (costs, security of the state, private interests, etc), there are a number of elements, particular to Switzerland, that make the application of transparency laws even more complicated. That does not mean that transparency is impossible, au contraire, but simply that these challenges must be recognized and addressed in establishing the basis of freedom of information. Of all these challenges, two are of particular importance: 1) the principle of collegiality, and 2) the principle of executive federalism.

Collegiality

The federal executive is made up of 7 members coming from 4 different political parties (from populist right to socialists). It is the principle used in reaching a decision in this politically diverse executive that differs from other democratic countries used to a principle of majority governments and parliamentary opposition. The Federal Council takes all of its decisions as one and applies the concept of collegiality (Constitution, 1998: Art. 177; Klöti, 2004). This means that decisions, after having been debated among the 7 members of the government, must then be defended by all, even by those who opposed it in the confines of the Council. Those who had to rally to the majority do not make their opposition public, and hence would prefer to keep private their own argumentation on the case.

There thus remains, at the heart of the political system, a zone of secrecy, shared by members of various political families. This particular configuration thus gives, at least at the executive level, a broad access to information to a representative of all major political parties and, consequently, gives everyone a certain stake in the preservation of secrecy. That being said there nevertheless remains a number of smaller parties that are represented in Parliament but that are not in the executive. In that decision making process, two steps must be distinguished: the procedure of 'co-rapport' and the consultation phase. They both have direct influence on the development and understanding of access to information.

The procedure of 'co-rapport' refers to all the documents written by the government and their staff following a proposition made by one the 7 members of government. These reports are then circulated between departments, at various levels of the hierarchy, for feedback. In such a system, the opening to all of the inside workings of the government would be problematic, and shake the basis of the concept that has served as the foundation of Swiss politics for decades.

The second level in the production of opinion within the Swiss federal government is the consultation of the various offices or departments. In the process leading to the preparation of the proposals devised by the Federal Council, the responsible administration invites the other administrations impacted by the proposal to give their input. It is based, in part, on these documents that the Federal Council will take its decision. The right to access to this information does exist, but only after the decision has been made.

Other, if not most jurisdictions do protect the formation of opinion at the center of government; nevertheless, the Swiss case is probably the only one where the process is so central to the very configuration of the governmental architecture.

Executive federalism

The second element touches the federal structure of Switzerland and, most particularly its 'fédéralisme d'exécution' or executive federalism (Kissling-Näf and Wälti, 2004). Contrary to most federal states, the central government does not carry-out all of its decisions, but rather delegates this task to the various Cantons - it is implementation by federal delegation (Linder and Vatter, 2001). Such a system ensures a greater level of adaptation of the legislation to the particular realities of each Canton. This structure also entails numerous interactions between the various levels of government, and most of these governments do not yet have legislation on access to information. The level of transparency wished by some might not, is not, welcomed by all (Busslinger, 2004). This in fact resembles the challenges posed by networked governance and transparency laws in institutions such as the European Union, the United Nations and the World Bank (Bunyan, 2002; CPA and Association, 2004; Roberts, 2002a). To make sure that information provided by the Cantons do not 'escape' the federal attempt at transparency, which would cover a very large number of federal documents and hence diminish the effectiveness of the legislation, the LTrans applies to all documents held by the federal administration, be they produced by or simply have been communicated to it.

These elements do account, in a certain measure, for the relative lateness of the introduction of access to information in Switzerland. Now that the LTrans has come into effect, it is interesting to note that these institutional elements have been taken into account in the construction of a transparency à la Suisse.

The main elements of the Swiss LTrans

Laws on access to information always have relatively similar characteristics (Frankel, 2001). Among those, we shall underline the important elements pertaining to the coverage of the law (what organisations and what type of documents), exceptions (what is officially off line), the practicalities (how to use it) as well as its regulatory framework (appeal process).

Coverage

The law will cover the totality of the federal administration as well as other organisations as long as they provide decisions of 'first instance' (decisions based on federal public laws and which, inter alia, create or modify rights or obligations or rule on the existence and extent of rights and obligations.) With this principle in place, state enterprises active on private markets will come under the Law for all the decisions that they give in their role as public authorities.

However, the Law does not apply to a number of institutions, notably: the Swiss National Bank, the Federal Banking Commission, the Federal Assembly, Parliamentary Commissions and the Federal Council (LTRANS, 2004: Art.2). Moreover, Parliament can also effectively withdraw from the obligations of the Law particular administrative units or organisations if their mandates require it, if it might possibly damage their competitive position or if their tasks are deemed to be of minor importance (LTRANS, 2004: Art.2, al.3). The flexibility given to the authority on this matter appears to be quite consequent.

Only completed official documents are to come under the Law. For the LTrans, an 'Official Document' must meet with all three of the following criteria (LTRANS, 2004: Art.5) :

1. The information has been registered on a specific support;
2. the information is located within a specific administration;
3. the information is linked to the execution of a public task.

The first of these cumulative criteria aims at distinguishing between the concept of document and the larger concept of information. It refers to a report, an expertise, statistics, visual or audio documents, electronic sources, etc. The second criteria aims at ensuring that the administration can effectively access the information requested. The third element, the link to a public task, means that it must not be linked to a general notion of public interest, but rather to an effective task carried out by the Confederation (Conseil fédéral, 2003: 1834-1838).

Documents that are not in their definitive state or that are destined to a personal use are not subjected to the Law (LTRANS, 2004: Art.5, al.3). The idea behind this provision is to ensure

that the administration retains the possibility to modify projects and avoid misunderstandings and external pressures based on draft documents (Conseil fédéral, 2003: 1840). Of course, the concept of what is and what is not a 'definitive state' will have to be validated and tested with use.

That being said, a personal letter regarding official information will be subject to the Law (Conseil fédéral, 2003: 1840). Documents sold by an organisation (maps, books, statistics, etc) are not considered official documents in the application of the Law (Conseil fédéral, 2003: 1839).

The law will not cover access to documents related to legal procedures, be they civil, criminal or linked to international cases. Moreover, information linked to personal data will still be protected by the Federal Law of June 19th 1992 on Data protection (LPD, 1992: Art. 3,9,11,12). By personal data is meant inter alia, data related to opinion (religious, political, etc), elements touching health related matters, or any assemblage of information allowing for the appreciation of one's personality or physical traits.

Exceptions

The right of access can be legally limited, delayed or refused for different reasons. These reasons are somewhat similar to those used in other jurisdictions (Canada, 1985; Frankel, 2001; Ireland, 2003).

As we have seen, access can be refused if the document is susceptible to hamper the free formation of opinion (LTRANS, 2004: Art.7, al.1). By protecting the formation of opinion, the legislation aims at preventing the premature dissemination of the government's position, thus insuring its ability to develop positions without the pressure of the media or the population.

Disclosure can also be blocked if the document is deemed to potentially compromise the relations between the Confederation and the Cantons or the relations between Cantons (LTRANS, 2004: Art.7, al.1e). This is a crucial element for most of the Cantons have no legislation on transparency. Unfortunately it also means yet one more area where transparency will not be applied.

As well, disclosure will be refused when the document could compromise internal or external security, the interests of Switzerland in terms of foreign, economic or monetary policy, as well as in terms of foreign affairs or international affairs (LTRANS, 2004: Art.7, al.1c,d,f). This aspect is particularly important as it has been shown in other jurisdictions to be used as a trump card in favour of secrecy (Blanton, 2003; Canada, 1994; Canada, 2004; Pasquier and Villeneuve, 2004; Pasquier and Villeneuve, 2005; Roberts, 2003). The terminology between

jurisdictions does vary, but the concepts surrounding notions of 'international relations' are, in the case of access to information laws, always framed in the most imprecise way, thus creating additional wiggling room to 'hide' information. This situation is likely to get even more acute as multi-lateral fora multiply and international agencies regulate more and more sectors of activities.

The non-disclosure of information is allowed when that information has been given by a third party to an organisation that has guaranteed its secret (LTRANS, 2004: Art.7, al.1h). This particular elements means, among other things that secret information passed on by other governments will not be accessible. This provision does not apply to information provided by individuals as part of a legal obligation (Conseil fédéral, 2003: 1853).

The standard protection is guaranteed for element that could lead to the release of professional, business or patent information(LTRANS, 2004: Art.7, al.1g). As well, a document might be withheld if it might damage private interests, unless an overriding public interest is found to exist (LTRANS, 2004: Art.7, al.2).

Nevertheless, all these cases of predominant interest (public or private) must always be balanced with the overriding public interest of transparency. As we can see, these exemptions are not unprecedented, for most of them can be found in other jurisdictions. Nevertheless, they were carefully crafted to ensure the protection of some of the Swiss specific mechanisms such as the concept of collegiality and Federal-Cantonal negotiations. It remains to be seen whether all these limitations will have a large or small impact on the benefits of transparency.

Practicalities

The requests for information must be directly addressed to the authority in charge of their production, and be as precise as possible (LTRANS, 2004: Art.10). The access is fee based; nevertheless, no fee will be collected for demands that entail small expenses for the administration or that are directly linked to mediation procedures. Overall, it is the Federal Council that will establish the modalities and tariffs to be charged (LTRANS, 2004: Art.10).

The time limit afforded to the organisation is 20 days starting with the day the demand has been received. The time provided to reply can be exceptionally extended if the demand requires more work in terms of volume or in terms of complexity (LTRANS, 2004: Art.12).

Regulatory framework

As with most freedom of information legislation, the Swiss Law has provisions to deal with complaints on the non-compliance with the law. A citizen can ask for mediation if the demand has been limited, delayed or refused (LTRANS, 2004: Art.13, al.1). The demand for mediation

must be presented to the 'Préposé fédéral à la protection des données et à la transparence', the Officer in charge of data protection and transparency, within a delay of 20 days starting at the reception of the decision.

This is, first and foremost, a mediation procedure where the 'Préposé' will try to reconcile the differences. It is hoped that this mediation approach will help take care of the bulk of demands without having to systematically resort to a more demanding system. This 'Préposé' is an independent agent that is not under the hierarchical purview of the Federal Council. He also has the use of his own secretariat. It is to be noted that the 'Préposé' has no power to force a decision. Aside from its role as supervisor of the Law and authority, the 'Préposé' is charged with the evaluation of the Law and with presenting an annual report to the Council on its application. More than only taking care of mediation, this 'Préposé' is in a sense a competency center on questions of transparency (Conseil fédéral, 2003: 1869).

A failure of the mediation process can subsequently be taken to the federal Commission on data protection and transparency. The Commission has the same provision as the Préposé in terms of independence. In such a case the Commission would have access to the documents, even if they are deemed secret. The Commission has to reach a decision within 2 months. This decision is not final, as it can be appealed to Federal Tribunal, the highest authority in Switzerland.

Final dispositions

Interestingly, the present legislation only covers official documents that have been produced or received after the enactment of the legislation (LTRANS, 2004: Art.23). That means that contrary to the situation with the new information legislation in the United Kingdom and the statutes in most countries with freedom of information regimes, no document from previous administrations will be accessible (Happold, 2005).

Conclusion

Overall, the LTrans is somewhat similar to other freedom of information legislations around the world. The great difference is of course the attempt made to accommodate some of the particular institutions of the country such as the federal-cantonal relations and the concept of collegiality. It remain to be seen if these attempts at adapting transparency to the local socio-political institutional arrangements are necessary cultural modulation of transparency, or simply a convenient way of deflecting the full glare of transparency's lights.

The impact of various legal provisions on the overall transparency of an administration have been analysed by numerous scholars. Of all these analysis, covering most continents, and

various administrative systems, one can only conclude that it is truly the practice that they succeed or fail to yield all the benefits of transparency. The overall consequences for Swiss public administration are likely to be positive. But, as of now, few seem to be aware of this new legislation, and fewer still aware of the cultural revolution it is likely to entail for the whole system.

In its capacity to adapt to this new reality, Switzerland will prove a testing ground for transparency. Of particular interest will be its ability to face not only an administrative cultural revolution, but one that also goes against a more generalised social conception of the role and function of the state.

In the opening remarks of the inaugural issue of Open Government, Steve Wood mentioned the impressive reporting on the Freedom of Information Act in the United Kingdom. It is to be hoped that after a few months, Swiss citizens will be as adept as the British at using transparency to its fullest.

References

LPD - Loi fédérale sur la protection des données, 1992 (235.1), Swiss Federal Parliament

LIn - Loi sur l'information du public, 1993 (107.1), Parliament of the Canton of Bern
Constitution Suisse, 1998, Swiss Federal Parliament

LIPAD - Loi sur l'information du public et l'accès aux documents, 2001 (A 2 08), Parliament of the Canton of Geneva

LInfo - Loi sur l'information, 2002 (170.21), Parliament of the Canton of Vaud

Loi sur l'information et l'accès aux documents officiels 2002 (170.801) Parliament of the Canton of Jura

LTRANS - Loi fédérale sur la transparence de l'administration, 2004 (03.013s), Swiss Federal Parliament

Banisar, D. (2004) The www.freedominfo.org global survey: freedom of information and access to government record laws around the world. [Accessed 01/05/06]

Blanton, T., Fuchs, M. & Elias, B. (2003) Justice Delayed is Justice Denied: The Ten Oldest Pending FOIA Requests. Washington, DC 20037, The National Security Archive.

Blanton, T. S. (2003) National security and open government in the United States: Beyond the balancing test. In: National security and open government: striking the right balance. New York, The Maxwell School of Syracuse University.

Bunyan, T. (2002) Secrecy and openness in the European Union. Freedominfo.org. [Accessed 01/05/06]

Busslinger, L. (2004) Tout savoir sur les salaires des fonctionnaires romands? Le rapport existe, mais il est top secret. Le Temps. 2109 ed. Genève.

Caddy, J. (2001) Access to Information. Paris, OECD.

Canada, Commissaire à l'information du (1994) La loi sur l'accès à l'information. Dix ans d'accès à l'information. Vers l'avenir... Ottawa, Travaux publics et des services gouvernementaux Canada.

Canada, Commissaire à l'information du (2004) Rapport annuel du Commissaire à l'information 2003-2004. Ottawa, Commissariat à l'information du Canada.

Loi sur l'accès à l'information, 1985 (L.R., 1985, ch. A-1), Parlement du Canada

Conseil Fédéral (2003) Message relatif à la loi fédérale sur la transparence de l'administration.

Cpa & Association, C. P. (2004) Recommendations for Transparent Government. Accra, Commonwealth Parliamentary Association and the World Bank Institute.

Frankel, M. (2001) Freedom of information: some international characteristics. Transparency in Europe a Conference. The Hague.

Happold, T. (2005) Major calls for election halt to FoI. The Guardian. 10 February 2005 ed. London.

Hasan, I. (2005) The UK Freedom of Information Act (2000) and Procurement. Open Government: a Journal on Freedom of Information, Vol. 1. www.opengovjournal.org

Héritier, A. (2003) Composite democracy in Europe: the role of transparency and access to information. Journal of European Public Policy, Vol. 10.

Ireland, Information Commissioner of (2003) Annual Report 2003. Dublin, Office of the Information Commissioner.

Kissling-Näf, I. & Wälti, S. (2004) The implementation of public policies. In: Klöti, U., Knoepfel, P., Kriesi, H., Linder, W. & Papadopoulos, Y. (Eds.) Handbook of Swiss Politics. Zurich, Neue Zürcher Zeitung.

Klöti, U. (2004) The Government. In: Klöti, U., Knoepfel, P., Kriesi, H., Linder, W. & Papadopoulos, Y. (Eds.) Handbook of Swiss Politics. Zurich, Neue Zürcher Zeitung.

Kriesi, H. (1998) Le système politique suisse, Paris, Economica.

Linder, W. & Vatter, A. (2001) Institutions and outcomes of Swiss federalism: The role of the Canton in Swiss politics. West European Politics, Vol. 24.

Mendel, T. (2003a) Freedom of information legislation: progress, concerns and standards. In: Transparency international (Ed.) Global Corruption Report 2003. Berlin.

Mendel, T. (2003b) Freedom of Information: a comparative legal survey, Paris, OECD.

OECD (2002) Public sector transparency and accountability: Making it happen. Paris, OECD.

Pasquier, M. & Villeneuve, J.-P. (2004) Les entraves politiques et administratives à la transparence gouvernementale. Revue économique et sociale, décembre 2004.

Pasquier, M. & Villeneuve, J.-P. (2005) Typologie des comportements organisationnels des administrations publiques visant à limiter l'accès à l'information. Working Paper IDHEAP. www.idheap.ch [Accessed 01/05/06]

Roberts, A. (2002a) Multilateral Institutions and the Right to information: Experience in the European Union. European Public Law, Vol. 8.

Roberts, A. (2002b) New Strategies for Enforcement of the Access to Information Act. Queen's Law Journal, Vol. 27.

Roberts, A. (2003) NATO, secrecy and the right to information. East European Constitutional Review, Fall/Winter 2002-2003.

Sanchez, A. C. (2002) The right of access to information and public scrutiny: transparency as a democratic control instrument. In: OECD (Ed.) Public sector transparency and accountability: making it happen. Paris, OECD.

Author: Dr. José Angel Martínez Usero, Library and Information Science Department
Universidad Complutense de Madrid

Title: Evolution of freedom of information related law in Spain: new prospects for a more open government

Volume 2 issue 2

Abstract

The evolution of FOI law in Spain over the last 30 years is analysed. The process starts with the Constitution of 1978 and goes on with a series of FOI related laws on the management of public administration services, the automatic processing of personal data, the access to environment information, as well as other technological legislation. This legislative package in some ways has contributed to foster and improve freedom of information in the Spanish public and private context. It is concluded that the right to general access of public information in Spain is totally guaranteed but it should be properly recognized with a specific law. Nevertheless, at present Spain lacks a real "Freedom of Information Act".

Introduction

It is now widely recognized that the culture of secrecy which has been a normal way of working of governments for centuries is no longer feasible in the present information and knowledge society. Governments in the knowledge society must provide information to be considered efficient. So, the transformation has begun and it is no longer possible to tell citizens that they have no right to know. As a result, a new era of government transparency is being promoted.

Access to government records and information is an essential requirement for modern government. Access facilitates public knowledge, democratic participation and discussion. It provides an important guard against abuse, mismanagement and corruption. It can also be beneficial to governments themselves – openness and transparency in the decision making process can assist in developing citizens' trust in government actions and in maintaining a civil and democratic society.

The main factor for the adoption of freedom of information (FOI) related laws in Spain was the transition from dictatorship to democracy in 1975 with the publication of the Spanish Constitution in 1978, as well as the process of modernization and adaptation to the new information society principles. Therefore, there is a double reason for FOI laws: a political approach due to the change in government form and a technological perspective provoked by

the expansion of the Internet into everyday life which has increased demand for more information by the public, businesses and civil society groups. Inside governments, the need to modernize record systems and the move towards e-government has created an internal constituency that is promoting the dissemination of information as a goal in itself.

The main objective of this article consists of analysing the most important legislative texts related to FOI passed in Spain and providing an up-to-date assessment of the present situation on freedom of information in Spain.

The Constitution of 1978

The current Spanish Constitution was passed in 1978 and was inspired by the desire to make Spain an advanced society. Its preamble proclaims the will of the Spanish people to "establish an advanced democratic society" and "promote the cultural and economic progress in order to ensure a worthy quality of life for all". So the Spanish Constitution can be identified as the basis for freedom of information legislation in Spain. In this context, it is worthwhile analysing some of its articles relating to information access.

In Article 20.1d the right to know is recognized as one of the "fundamental rights and public freedoms". The article establishes the right to "freely communicate and receive true information through any medium of dissemination. The law shall regulate the right to invoke the clause of conscience and professional secrecy when exercising these freedoms". This article tries to make very clear that the law will not tolerate the systematic infringement of the principal of transparent information practiced by the former regime (Cornella, 1998).

Article 20.2 establishes that "the exercise of these rights cannot be restricted by any form of prior censorship". Villaverde (1995) has discussed Article 20.1.d. at length, maintaining that its recognition of the right of access to "true" information is one of the keys to the democratic system. But from the standpoint of information, the article is not very clear as this "right to be informed" is directly linked to communications media, regardless of their type. In other words, it appears that legislators were more concerned with establishing a principle that would prevent prior censorship than in recognizing the general principle of the right of access to information.

Article 105.b states that the Constitution is not clear on public rights to information. This article deals with public access to government information and begins with the controversial statement, "the law shall regulate" rather than clearly stating that what follows is a fundamental right. It specifies that "[the law shall regulate] public access to government archives and registers, except in those cases in which access would jeopardize State security

or defence, the investigation of crimes, or individual privacy". This article is developed in the Law of 1992 on Rules for Public Administration which will be discussed further on. Suffice it to say here that guaranteeing public access to government information does not necessarily mean that government agencies have a duty to actively disseminate the information in their power.

Article 18.3 establishes that "the secrecy of communication, particularly via postal, telegraph and telephone services, shall be guaranteed unless a court decision is made to the contrary". In a similar way, Article 18.4 establishes that "the law shall limit the use of computerized information in order to guarantee the honour and privacy of all citizens and their families and the full exercise of their rights".

As mentioned above, Article 105.b of the Spanish Constitution states that "[the law shall regulate] public access to government archives and registers, except in those cases in which access would jeopardize State security or defence, the investigation of crimes, or individual privacy". But it is not clear from the wording of the article whether it recognizes that the public's right of general access to information is a principle as described above, or if it is a supplementary right of the democratic system, which guarantees that people with a legitimate interest (because they are involved in a court case, for example, or because the files contain personal information about them) can have access to government files. From the citizen's viewpoint, the important matter is what information can be consulted and by whom. In order to reply to these questions, the Law 30/1992 of November 26th, on Rules for Public Administration, which specifically governs the right of access to public archives and registers, is going to be analysed.

The 1992 Law on Rules for Public Administration

This law regulates the access to government records and documents by Spanish citizens and includes rules for the access of persons to administrative proceedings.

In accordance with this law, documents can be withheld if the public interest or a third party's interest would be better served by nondisclosure or if the request would affect the effectiveness of the operations of the public service. Access can also be denied if the documents refer to government actions related to constitutional responsibilities, national defence or national security, investigations, business or industrial secrecy or monetary policy. Access to documents which contain personal information is limited to the persons named in the documents. There are also restrictions for information protected by other laws including classified information, health information, statistics, the civil and central registry, and the law on the historical archives (Banisar, 2004, p.80).

The denial of access to information accessing can be appealed administratively. Therefore, Public Administration is also required to maintain a registry of documents and to publish rules and decisions.

Article 35.a of this law recognizes the right of private citizens "to know, at all times, the status of any procedures in which they are interested parties and to obtain copies of any documents forming part of these procedures". It thus becomes imperative to define what is meant by an interested party. The answer is found in Article 31, which states that "interested parties in administrative procedures are considered as a) those who institute such proceedings by virtue of their individual or collective rights or legitimate interests ; b) those who have not instituted the procedure, but have rights which may be affected by the decision made, and c) those whose individual or collective legitimate interests could be affected by the decision and who appear in the court proceedings before a final decision has been made". This article thus guarantees the right of access to public information as specified above, but does not guarantee the right of general access to public information (Cornella, 1998).

Furthermore, Article 35.h recognizes the right of "access to government registers and archives on the terms established in the Constitution and in this or other laws". For a better understanding of this article, it is necessary to analyse Article 37.1 which states that "citizens have the right of access to the registers and documents which are contained in government archives as part of a file, regardless of the form of expression, written, recorded or in image, or the type of medium in which they appear, provided that these files refer to proceedings concluded by the date of application". The subsequent paragraphs of Article 37 specify the exceptions to this right, which are aimed basically at safeguarding the public interest and individual privacy. The wording makes it difficult to interpret it as establishing a principle of general access to public information; first, because it never clearly defines the meaning of "file" and second, because access is limited to files which have already been closed.

Lastly, it should be noted that Article 38.3 of the law stipulates that "general registers, as well as all government records of documents and correspondence received from private parties or government agencies, should be stored in an electronic format". That is to say, the law recognizes that information technologies should be used to manage registers. This may indicate that the law is still more concerned with computer infrastructure than with using information technologies to guarantee the public's general access to government information.

The 1992 Organic Law on Automatic Processing of Personal Data

Organic Law 5/1992 of October 29, on Automatic Processing of Personal Data (LORTAD), which generally aims to establish a regulatory framework that prevents unlawful trade of personal data in possession of either the public or private sector.

The LORTAD is based on a series of principles related to freedom of information that are mentioned in the following paragraphs:

- Files containing personal data cannot be used for any purpose other than that for which they were originally intended, except with the consent of the parties concerned.
- Personal data contained in files should be "accurate and up-to-date".
- All citizens have the right to know what information is contained in their files and to correct or cancel registrations in which such data appear.
- Protection of certain data is particularly strict: opening files for the exclusive purpose of storing personal data that reveal ideology, beliefs, race or social status is strictly prohibited and inclusion of any of such data in any file must be expressly authorized in writing by the parties concerned.
- Those people responsible for files containing personal data must take the security measures necessary to ensure that such data will not be lost, altered or handled without authorization, and undertake to keep them a professional secret.

Article 11 is particularly important as it stipulates the conditions under which creators of files containing personal data are permitted to assign rights of these files to a third party. Under the terms of the article, "personal data...may only be assigned [to third parties] for purposes directly related to the legitimate activities of the assignor and the assignee and with the prior consent of the party concerned". There are, of course, a number of exceptions (as, for example, when the information is taken from public sources such as telephone books). Paragraph 3 of the article specifies that "the consent [of the party concerned] will not be valid unless it is given to a specific or specifiable assignee or if the purpose of the assignment is not clearly stated".

Article 19 prevents government departments from interchanging data for purposes other than those for which the data files were originally created.

It is evident that one of LORTAD's principal objectives is to prevent trading in personal data, whether by publicly or privately owned organizations or bodies. Before the law came into effect such transactions were quite common in Spain. Moreover, some years later, in 2002, the Law on Information Society Services and Electronic Commerce would establish some specific criteria for the usage of personal data and their management in an electronic environment.

Law 38/1995 on the right of access to information relating to the environment

This law implements the European Directive 90/313/EEC on Access to Environmental Information, repealed by Directive 2003/4 of 28 January 2003. It was adopted after the European Commission found that the above mentioned Law on Public Administration was not adequate and started infringement proceedings against Spain in 1992. The incorporation of Spain to the European Union thus fostered the adoption of European legislation related to access to information and it can be considered of benefit to Spanish citizens and business.

The 1998 General Telecommunications Law

The obligation imposed by the European Union to liberalise telecommunications, coupled with the growing proliferation of information dissemination technology, forced the Spanish government to establish various rules and regulations to get rid of the telecommunications monopoly without ceasing to offer this public service. Therefore, after having produced specific rules and regulations to liberalise the telephone service, the use of different types of technology was promoted (Caridad, 2001, p. 54).

Some of the main important objectives of this law are linked to the freedom of information and equal access to telecommunication services, such as:

- a. To grant the administration the faculties needed to ensure free market conditions favouring the people's right to access universal information services.
- b. To regulate the public service obligations of the public network operators, in order to guarantee the protection of general interests in the liberalised market.
- c. To distribute competence on telecommunications among the various bodies of Spain's State Administration.
- d. To make the rates applied to these technological services uniform.

This and other laws to this respect have led to the existence of several telecommunications operators in Spain, thereby allowing for a decrease in prices and the opportunity to select various forms of access to telecommunications services, including the Internet, from among different operators and access providers. That is to say, offering a better access to information services.

The 1999 Organic Law on the Protection of Personal Data

This is the Spanish law that would be equivalent to a "Data Protection Act" which allows individuals to access and correct records about themselves held by public and private bodies. It is worthwhile pointing out some relevant articles related to freedom of information topics. Article 4 establishes that personal data shall be stored in a way which permits the right of access to be exercised, unless lawfully deleted.

Article 15 is concentrated on the right of access and regulates that the "data subject shall have the right to request and obtain free of charge information on his personal data subjected to processing, on the origin of such data and on their communication or intended communication". Moreover, "the information may be obtained by simply displaying the data for consultation or by indicating the data subjected to processing in writing, or in a copy, fax or photocopy, whether certified a true copy or not, in legible and intelligible form, and without using keys or codes which require the use of specific devices.

Article 28 refers to data included in sources accessible to the public. In this field, the law regulates that personal data contained in the publicity register or on the lists of persons belonging to professional associations must be limited to those strictly necessary to fulfil the purpose for which each list is intended. The inclusion of additional data by the bodies responsible for maintaining these sources shall require the consent of the data subject, which may be revoked at any time. Furthermore, data subjects shall have the right to require the body responsible for maintaining the lists of professional associations to indicate, free of charge, that their data may not be used for the purposes of publicity or market research.

Finally, this law is enforced by the Spanish Data Protection Authority, also called Data Protection Agency, which is considered a body under public law, with its own legal personality and unlimited public and private legal capacity, which acts fully independently of the public administrations in the performance of its duties.

The Spanish Ombudsman's opinion

The Ombudsman recommended in 2002 that agencies make access with 15 days for files for with an interest and 30 days for general access and not overuse the exception on effectiveness of the public administration. Government bodies are also required to maintain a registry of documents and publish acts and decisions. But unfortunately, this situation is not always accurate.

An extensive report published in October 2005 by Sutentia and The Open Society Justice Initiative concludes that nearly 60 percent of the requests filed under the Law 30/1992 for the study were unanswered. From requests filed under the Law 38/1995 on the right of access to information relating to the environment, only 30 percent were answered correctly, while 20

percent were answered late and the remaining 50 percent were never answered. The report recommends that Spain needs to adopt a FOI law according to international standards because Law 30/1992 is not enough to guarantee an adequate right of access.

There was considerable controversy about information over the blame for the 11 March 2004 Madrid train bombings. The government selectively declassified documents in March 2004 after it lost the election in an effort to show that ETA was responsible for the bombings. The Prime Minister, Jose Luis Rodriguez Zapatero said in December 2004 that his predecessor Jose Maria Aznar had destroyed all computer files relating to the investigation of the bombings when he left office. Zapatero received the €12,000 bill by the computer consulting firm for the destruction of the files (Banisar, 2006). Therefore, this is an example on the big gaps that future Spanish law on FOI should cover.

Other legislation related to freedom of information

Once mentioned the most relevant Spanish legislation related to freedom of information, it is worthwhile pointing out some other legislation which includes specific topics linked to freedom of information and which can be used to provide a better assessment of the present situation in Spain (IDABC, 2005). In the last few years Spanish law has undergone a huge development in different technological fields, such as: e-commerce, e-communication, e-government and e-signatures. Nevertheless, a freedom of information act has not been developed.

In the field of **e-commerce legislation**, the Law 34/2002 on Information Society Services and Electronic Commerce of July 11th, 2002 implements the EU E-Commerce Directive (2000/31/EC).

The law states that the operators of electronic communications networks and services and the service providers may not use the data held there under for purposes other than those indicated in the paragraph below or other purposes permitted by the Act and must take appropriate security measures to avoid the loss or alteration of such data and unauthorised access to such data.

Article 21 on prohibition of unsolicited commercial communications through electronic mail or equivalent means of electronic communication establishes that it is prohibited to send advertising or promotional communications by electronic mail or another equivalent means of electronic communication when not solicited or expressly authorised in advance by the recipient of the communications. Moreover, article 22 includes that "when service providers employ devices for the storage and recovery of data from terminal equipment, they shall

inform recipients of the use and finality of such devices in a clear and comprehensive manner, offering recipients the opportunity to refuse, by a simple means and free of charge, to allow their data to be processed”.

In the field of **e-communications legislation**, the General Telecommunications Law 32/2003, of 3 November 2003, implements into Spanish law the new EU regulatory framework for electronic communications. Transposition was completed with the adoption of the new Regulation on electronic communication markets in December 2004.

Article 33, dedicated to secrecy of communications, holds that operators who run public electronic communications networks or deliver publicly available electronic communications services must guarantee the secrecy of communications in accordance with articles 18.3 and 55.2 of the Constitution and must therefore take the necessary technical measures accordingly.

Article 34 on personal data protection establishes that operators who run public electronic communications networks or deliver publicly available electronic communications services must guarantee that in the exercise of their activity personal data is protected pursuant to current legislation.

The operators to which the paragraph above refers must take the appropriate technical and management measures to uphold security in the operation of their network or in the delivery of their services, with the purpose of guaranteeing the levels of personal data protection required by the rules implementing this Act on this matter. Where there is any particular danger that the security of the public electronic communications network may be violated, the operator running said network or delivering the electronic communications service shall inform subscribers of said risk and the measures that should be taken.

In the field of **e-government legislation** it is important to point out that there is currently no overall e-government legislation in Spain. However, a number of decrees regulate generic aspects of the development of e-government in the country, in particular Royal Decree 263/1996 of 16 February 1996 on the use of electronic and telematic techniques in the public administration (modified by Royal Decree 209/2003 of 21 February 2003 on the use of telematic registers and notifications and of electronic certificates) and Royal Decree 589/2005 of 20 May 2005 on the organisations in charge of electronic administration.

E-government services represent an opportunity for improving access to public information, achieving administrative transparency and more intensive citizen participation. Nevertheless, as the implementation of e-government services in Spain is based on efficiency and economic

criteria, the development of different services is not equal. Thus the Spanish e-government fiscal services are the most developed and sophisticated in Europe, and an example to other countries (Lara, 2002). It can be said that e-government legislation is helping to take into consideration more freedom of information resources, but its implementation is not based on general access to information criteria.

In the field of **e-signatures legislation**, the Law 59/2003 of 19 December 2003 on Electronic Signature replaced a Royal Decree of 1999 on Digital Signatures. It transposes the European Directive 1999/93/EC on a Community framework for electronic signatures, and is aimed at promoting a widespread use of electronic signatures for e-commerce and e-government. Amongst other provisions, the law clarifies relevant concepts and terminology, introduces an electronic signature for legal entities, promotes certification industry's self-regulation, establishes a legal framework for the future development of a national electronic ID card and regulates the electronic access to public information services.

Conclusions

The legal situation in Spain from the late 70s to the early years of the twenty first century has undergone very deep changes. A series of laws on the management of public administration services, the automatic processing of personal data, the access to environment information, as well as other technological legislation related to freedom of information has been passed. This package of legislation provides a clear idea of the present situation in Spain. It is important however to highlight the fact that Spain lacks a real "Freedom of Information Act".

If the right of general access to public information in Spain is to be properly recognized and guaranteed, the country probably needs a specific law, similar to other European countries. Spain is one of the few countries in Europe that does not have a dedicated access to information law. Monitoring studies, notably that carried out by the Open Society Justice Initiative and Sustentia in 2004, have shown that the current provisions of administrative law are failing to guarantee the right to information.

The lack of a specific FOI law is hindering the development of the information industry in Spain, preventing it from occupying a position consonant with that of the country's economic position on the world stage. The main reason for this is that in Spain, as in the most other countries, the public sector is the principal producer of information, much of which cannot be used without the participation of the private sector. Public-private synergies should be encouraged. But without a law on general access to public information, information will not be transparent enough to make this possible. That is to say, the inexistence of a specific FOI law can cause long term economic constraints on Spain's economy.

References

BANISAR, David. (2004) The Freedominfo.org global survey. Freedom of information and access to government record laws around the world. July 2006. [Spain], pp. 113-115. Available at: http://www.freedominfo.org/documents/global_survey2006.pdf [Accessed 4th August 2006]

CARIDAD SEBASTIÁN, Mercedes; RODRÍQUEZ MÉNDEZ, Eva; RODRÍGUEZ MATEOS, David. (2001) Information policies in Spain: towards a new information society. Libri, vol. 51, pp. 49-60

CORNELLA, Alfons. (1998) Information policies in Spain. Government information quarterly, vol. 15, n. 2, pp. 197-220.

General Telecommunications Law 32/2003 of 3 November 2003. (In Spanish: "Ley General de Telecomunicaciones").

IDABC. (2005) eGovernment Factsheet - Spain - Legal framework. EGovernment factsheet, November 2005. Available at: <http://europa.eu.int/idabc/en/document/1156/413>

LARA NAVARRA, Pablo; MARTÍNEZ USERO, José Ángel. (2002) Del comercio electrónico a la administración electrónica: tecnologías y metodologías para la gestión de información. El profesional de la información, vol. 11, nº 6, pp. 421-435. Available at: <http://www.ucm.es/eprints/5636/>

Law 34/2002 on Information Society Services and Electronic Commerce of 11 July 2002. (In Spanish: "Ley sobre Servicios de la Sociedad de la Información y del Comercio Electrónico").

Law 59/2003 on Electronic Signature of 19 December 2003. (In Spanish: "Ley sobre Firma Electrónica")

Organic Law 15/1999 on the Protection of Personal Data, of 13 December 1999. Available at: https://www.agpd.es/upload/ley_15_ingles_v2_pdf.pdf
(In Spanish: "Ley Orgánica de Protección de Datos de Carácter Personal").

Organic Law 5/1992 of 29 October 1992, on Automatic Processing of Personal Data. (LORTAD). (In Spanish: "Ley Organica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal").

Royal Decree 263/1996 of 16 February 1996, on the use of electronic and telematic techniques in the public administration (modified by Royal Decree 209/2003 of 21 February 2003 on the use of telematic registers and notifications and of electronic certificates)
Royal Decree 589/2005 of 20 May 2005, on the organisations in charge of electronic administration.

Spanish Constitution (1978). (In Spanish: "Constitución Española de 1978").

Spanish Data Protection Authority. (In Spanish: "Agencia Española de Protección de Datos").
Available at: <https://www.agpd.es/index.php?idSeccion=8>

Sustentia. (2005). "Transparencia y Silencio" Estudio Sobre el Acceso a la Información en España, Octubre de 2005. http://www.sustentia.com/transparencia_y_silencio_espana.pdf

VILLAVERDE MENÉNDEZ, Ignacio. (1995) Los derechos del público. El derecho a recibir información del Artículo 20.1.d) de la Constitución Española de 1978. Madrid, Spain: Tecnos.

Author: Marcus Turlle

Partner in the Privacy and Information Law Group at Field Fisher Waterhouse, UK

Title: Confidential and commercially sensitive information – stopping public Authorities releasing information in the UK (part 2 of an series of articles, part 1 published in Volume 2 issue 1)

Volume 2 issue 2

Compared with its overseas cousins, there are many facets of the UK's freedom of information regime which deserve celebration. The Freedom of Information Act 2000 (FOIA) is currently free to use (up to a point), applies to virtually all branches of government and, judged on the evidence of the last 18 months, has been fairly successful in blowing away the traditional culture of secrecy which had pervaded Westminster for decades. There is nevertheless one alarming omission from the UK rules which has brought unanimous condemnation from the supplier community: while most freedom of information regimes entitle third parties to receive notice when a public authority gets a request for their information (and some even allow them to participate in the decision whether to disclose), no such protections exist in the rules here.

In the US (whose freedom of information act turned 40 in July), companies can apply for a court order restraining disclosure – a process known as reverse-FOI. South African legislation requires public authorities to pay "due regard" to representations from companies. In both Canada and Japan, there is a notification obligation once a public authority has decided to release information. By contrast, FOIA contains nothing at all in the way of third party rights. This absence is strange given that third parties will often be better qualified to assess whether something is commercially sensitive, better informed about whether its disclosure would prejudice the regional economy and better able to appreciate the public interest arguments for maintaining an exemption. Nevertheless, the lacuna is deliberate. It reflects the view that third parties will naturally want to shield their information from public view. As a result, companies have no right to be consulted on how to answer a request, no right to be told when an applicant requests an internal review of an authority's refusal, no right to be notified that an authority has decided to disclose, no right to apply to the Information Commissioner for an adjudication on whether a decision to disclose is correct, no right to be consulted by the Commissioner when he is considering a challenge to a public authority's refusal, no right to be informed of any decision taken by the Commissioner ordering the release of information, and no right to appeal a decision of the Commissioner to the Information Tribunal. Companies do not even have a right to be notified when a public authority receives a request.

FOIA does contain 23 exemptions built into the Act, each one representing a specific interest which Parliament recognises as requiring special dispensation from the duty to disclose. Accordingly, FOIA provides exemptions for personal privacy (s.40), confidentiality (s.41) and commercial interests (s.43). (I examined ss.41 and 43 in my article last month.) Significantly, however, while ss.41 and 43 can operate to protect sensitive corporate information, this is always dependent on a public authority making use of them. FOIA never absolutely prohibits disclosure, even where an exemption is available – it merely offers a means of refusing to disclose if the authority so chooses. Furthermore, since many of the exemptions can only apply where the public interest allows, companies are reliant on a public authority's assessment of the factors for and against disclosure when forming a judgment on this. There is also of course the possibility that a public authority fails to appreciate the relevance of an exemption altogether, or simply discloses information inadvertently. So, given that relying for protection on the FOIA exemptions alone is such a perilous exercise, companies have a strong commercial and reputational interest in understanding what other means exist to prevent or limit the release of information which could be damaging.

The S45 Code of Practice

The Lord Chancellor's Code of Practice provides some help on the question of consultation. Paragraph 27 says that consultation with a third party will "in some cases ... be necessary" to determine whether an exemption applies or to reach a view on "whether the obligations in section 1 of the Act arise". The reference to s.1 is presumably intended to make it clear that authorities should consult on the public interest, although this must be implicit anyway in the earlier reference to the exemptions. The important point is that the word "necessary" does not impose an obligation. It is just a simple acknowledgment that informed and balanced decisions may be difficult without consultation taking place. The Code goes on to say that even where not actually necessary, consultation "will be good practice". Unfortunately, it recommends only that authorities take "reasonable steps...where appropriate, to give [third parties] advance notice [of disclosure], or failing that, to draw it to their attention afterwards".

Ultimately, however, the Code of Practice provides very limited comfort. First, its provisions are not legally binding. They are only indications of good practice which, in the opinion of the Secretary of State, it is desirable for public authorities to follow in discharging their FOIA obligations. Failure to comply can theoretically result in service of a Practice Recommendation by the Commissioner, but this is of no practical worth to a supplier who has suffered detriment from disclosure of sensitive information. Secondly, even where an authority does consult, it is not obliged to act on the representations it receives. The disclosure decision remains solely at the authority's discretion.

Court action

Companies always have the option of going to court to prevent a public authority disclosing something. Court action is fraught with practical and legal difficulties, however, and in the context of FOIA there is also the obvious matter of timing. Where an authority has ignored the recommendations for consultation in the Code of Practice (or worse, ignored its obligation to notify in the contract negotiated by the company), the information may already have been released when the company gets wind of the request (perhaps when a Times journalist calls to ask for comment on a story about the company's failure to live up to its service levels). The company may not, therefore, be in a position to apply to prevent the disclosure. Suing for damages after the event is a possibility, but the cost, uncertainty of outcome, potential liability for the authority's legal bill should the claim fail, and the difficulty of quantifying losses in the first place, make this something of a nuclear option. And it rarely makes business sense to drag a customer through the courts.

A supplier looking to prevent disclosure by an authority (or, indeed, to restrain an applicant who had obtained information under FOIA from making any further disclosure) could apply for an injunction. For an interim injunction, a company would normally have to make out its case on the balance of convenience (i.e. demonstrating that disclosure would cause it greater inconvenience than restraining disclosure would cause the public authority or the applicant). In a FOIA context, however, a higher test might apply – that of more likely than not to succeed at trial – given that an injunction pending a trial several months later could effectively deprive an applicant of their FOIA rights (if, for example, the value of the information will have disappeared by the time the trial takes place).

An alternative to full-on litigation is judicial review. It is arguable that public authorities, including the Information Commissioner and the Tribunal, have a duty to take proper account of third parties' views when deciding how to deal with a request for access to information. This could imply an obligation to consult. If so, then failure to do so could render a decision or order to disclose unlawful and liable to be quashed by the Administrative Court. The requirements for proper consultation have been established by the courts (it must take place when the decision is still at a formative stage, it must allow adequate time for consideration and response, and the product of the consultation must be conscientiously taken into account), but even a duty to consult does not imply a duty to obtain agreement before acting. There could be grounds for judicial review to challenge the decision of a public authority or a determination by the Commissioner or Tribunal where a decision was flawed by errors of law or fact, by substantive unfairness or unreasonableness, by unjustifiable inconsistency with earlier decisions or because supported by inadequate reasons, or because of a breach of the

Human Rights Act 1998. Bear in mind, however, that a different outcome will not necessarily result from a court ordering a public authority to reconsider.

A public authority could potentially be liable to a supplier if it disclosed information which was defamatory (that is, which lowered the supplier in the estimation of the public). Section 79 of FOIA precludes a claim for defamation if it was caused by a FOIA disclosure made without malice, but the immunity only applies to information which was supplied to the authority by another party. It does not therefore apply to allegations contained in papers generated by the authority internally, nor to FOIA applicants who further circulate the material. It is nevertheless extremely difficult to get a pre-publication restraining order on the basis of defamation because of the importance ascribed to free speech. Unless a company can show that an authority has no arguable defence (e.g. that allegations are substantially true or amount to fair comment), its options will normally be limited to seeking damages after the event.

The Information Tribunal

Since the advent of FOIA itself, rule 7 of the Information Tribunal (Enforcement Appeals) Rules 2005 has introduced an entitlement for third parties to apply to be joined as parties to any appeal against a Decision Notice of the Commissioner. Unfortunately, the practical value of this is limited because it is not open to a third party to appeal a Decision Notice in the first place (only the requestor or the public authority can do so), and there is no obligation on the parties to an appeal (nor on the Tribunal) to notify others. Where the third party does not itself apply to be joined to proceedings, the Tribunal may invite it to join. A third party which joins a Tribunal hearing is entitled (like the other parties) to lodge a further appeal to the High Court on a point of law.

Data protection

The Data Protection Act 1998 (DPA) provides various ways for individuals to prevent disclosure of personal data or to claim compensation following disclosure. Under s.10, a data subject can serve notice on a data controller requiring him not to disclose personal data where this would cause substantial and unwarranted damage or distress. Service of a s.10 notice would bring the information within the s.40(3)(a)(ii) exemption under FOIA provided the damage or distress claimed was valid. In addition, an individual could apply to the County Court for an order enforcing his s.10 notice, for an order under s.14 of the DPA to block disclosure or erase/destroy the data altogether, and for an order for compensation under s.13 of the DPA where disclosure had taken place.

Copyright

Some commentators have raised the possibility of preventing FOIA disclosure on the ground that disclosure would constitute an infringement of copyright (where a third party owns copyright in the information requested). The veracity of this remains uncertain. The Department for Constitutional Affairs has issued guidance stating that a public authority will not infringe copyright by responding to a FOIA request because it will be able to claim the defence of statutory authority (s.50 of the Copyright Designs and Patents Act 1988 (CDPA) permits copying where "specifically authorised by an Act of Parliament"). This does not quite hold true, however. FOIA requires information to be "communicated" but it does not specify how communication must be made. It does not therefore "specifically authorise" copying and so it is not clear that s.50 of the CDPA will apply, particularly where an authority could communicate information via a digest or summary, or by inviting an applicant to inspect a record. Further, a company may counter the DCA position by arguing that copyright material should be absolutely exempt under FOIA s.44(1)(a), which applies to information whose disclosure is "prohibited by or under any enactment" (in this case the CDPA), although this would seem to fall foul of the same point about copying as opposed to summarising or permitting inspection. In any event, it is unlikely in the author's view that the courts would countenance a position whereby the law of copyright automatically trumped FOIA because this would significantly impair the effectiveness of the Act in providing access to information.

Conclusion

The uncomfortable truth for suppliers is that they must live in hope that public authorities, the Commissioner and the Tribunal will invite them to participate in dealing with FOIA requests. And while there are potential sources of protection from the law outside FOIA, these are almost all problematic. Companies should recognise that the best protections against FOIA disclosure-risk continue to be a close and open relationship with public authority customers, the clear designation of information which may be exempt, contractual rights to be notified and consulted (including in relation to any Decision or Enforcement Notice, so that companies can consider scope for appealing or for applying to be joined as a party to an appeal), and communicating with the Commissioner in relation to any request which relates to their information, including if necessary drawing to the Commissioner's attention any failure by the authority to consult in accordance with the s.45 Code of Practice.

References

Copyright, Designs and Patents Act 1988 (c48) Available online at:

www.opsi.gov.uk/ACTS/acts1998/19980029.htm

Data Protection Act 1998 (c29) Available online at:

www.opsi.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm

Department for Constitutional Affairs (2004) Lord Chancellor's Code of Practice on the discharge of Public Authorities' Functions under the Part I of the Freedom of Information Act 2000. Issued under S45 of the Act. Available online at www.foi.gov.uk

Freedom of Information Act, (c.36). OPSI.

Available online at: <http://www.opsi.gov.uk/acts/acts2000/20000036.htm>

Information Tribunal (enforcement Appeals) Rules 2005. SI 2004/14 Available online at:

www.opsi.gov.uk/si/si2005/20050014.htm

Marcus Turler is a partner in the Privacy and Information Law Group at Field Fisher Waterhouse. He is the author of the definitive practitioner's guide to the UK's freedom of information regime, Freedom of Information Manual, published by Sweet & Maxwell (ISBN 0421922400).

Authors: Graham Sutton and Sarah Holsen
The Constitution Unit, University College London, UK

Title: China progresses information access and data protection laws

Volume 2 issue 2

The EU China Information Society Project is an initiative jointly funded by the European Union and the Chinese Government to promote economic and social reform in China through informatisation. Among other things, the Project aims to help China develop a regulatory infrastructure for the information society, including a legal framework on freedom of information and data protection, and to assist with the training of staff. This involves a two-way process, with experts from the EU working on short-term contracts in China alongside the small permanent staff based in Beijing, and Chinese officials visiting the EU to learn first-hand how things are managed here.

In June of this year we were invited by the Project to visit China as short-term experts to help with the work on freedom of information. Although we were well briefed in advance by the Project staff, it is fair to say that we did not really know what to expect. We were well aware of the struggle that had taken place in the UK before freedom of information became an operational reality. How much more difficult would it be in China? Two of our three formal commitments were traditional training seminars, for which we had been able to prepare presentations. But we had been told that no presentation was necessary for our first meeting, and we had no real understanding of what would be involved.

It turned out to be a workshop to discuss the draft of a national “regulation” (similar to a law, but passed directly by the State Council instead of the National People’s Congress) on “Access to Government Information” (as the FOI topic is usually referred to in China). It was presided over by Vice-Ministers from the two government offices most closely concerned with the preparation of the regulation – the State Council Legislative Affairs Office (SC-LAO) and the State Council Informatisation Office – with participation from senior officials and leading academics in the field. We were told that the workshop was part of the consultative process in the development of the law. We were invited to participate fully in the discussion, which was a great privilege, but difficult to carry out since the draft law was available only in Chinese. To follow the discussion we relied on one interpreter who translated all interventions throughout the day, both from Chinese into English and vice versa, (and, to her immense credit, never flagged). In practice, our role was limited to responding to questions about the position in the UK. The issues we were asked about included the fee regime, publication schemes, the need to protect internal government business, complaints about refusals to provide the information

requested, and the procedures for handling requests. Oh yes, and why did it take the UK five years to bring our law into force?

For our second meeting we travelled by train to Shijiazhuang, which is just south of Beijing and the capital of Hebei province. Our remit here was to give presentations about FOI in the UK and more generally in Europe (together with a colleague presenting about the German situation) at a seminar organised by the Hebei Informatisation Office. The day served as an introduction to the subject for local government staff from across the province. An interesting feature of the Chinese system is that laws and regulations, at least on matters of this kind, may be brought forward at both the national and local level. Hebei have it mind to legislate on freedom of information, and there was a great deal of interest in what we had to say.

Our final stop was Shanghai, which held a major surprise for us. Had we been told before going to China that China had an FOIA-like regulation in force before the UK we would probably have been rather sceptical. But the regulation containing Shanghai Municipal Provisions on Open Government Information was passed in January 2004 and brought into force in May of that year. We were told that other localities also have FOI provisions but it was not clear to what extent, if at all, the others are in force. In the light of their greater experience, it was with due humility, therefore, that we gave our presentations at a seminar for local government staff organised by the Shanghai Municipal Informatisation Commission.

Questions in both Shijiazhuang and Shanghai ranged very wide, but there was particular interest in the mechanisms for dealing with requests (where the questions suggested that the structure of government in China is very different from that in the UK) and the status and function of the Information Commissioner. Shanghai officials are clearly very proud of their city and its rapid development. They see FOI as being an essential complement to economic progress, since one of the reasons that they give for having an FOI regime is to help fight corruption. We were told by the Municipal government that about 95% of the local population are aware of the FOI regulation and that, by the time of our visit, there had been about 20,000 requests for information, mainly from private citizens.

In early September, about 10 Chinese officials, led by a senior member of the SC-LAO, came on a study visit to the EU under the auspices of the Project to see first hand how we manage FOI. They went first to Hungary and Germany, and then visited the UK, where the Constitution Unit organised a programme consisting of presentations at the Unit as well as visits to the ICO and National Archives. We were keen to give them the opportunity of hearing from a wide range of those involved with FOI - those who make requests, those who have to respond to them, academic commentators as well as those responsible for supervising the

legislation. We hope that the varied programme we laid on was both interesting and helpful. The only criticism we received was that it is a long way from London to Wilmslow!

Meanwhile, work continues in Beijing, not only on FOI but also on data protection (and a wide range of other topics related to Information Society). They are less well advanced in that field since they do yet have a draft law that they are willing to share with local experts. But one of the Project's activities is to help with the preparation and eventual implementation of a personal data protection law. In connection with that activity, I (Graham) was invited to return to Beijing in September. As well as speaking on data protection at the Project's annual conference, I took part in a workshop with academics and officials to discuss the key issues of concern in formulating a national data protection law, and a meeting with the Beijing Informatisation Office who are interested in bringing forward their own data protection law.

China is changing fast. Its economy is roaring ahead. It's encouraging that, with EU support, it is also working on the social measures that provide essential safeguards for its citizens as it races into the information age.

References

EU China Information Society Project <http://www.eu-china-infso.org/>

Book Review

Hood, C & Heald, D (eds) (2006) *Transparency: the key to better governance?* Oxford. Oxford University Press. ISBN 0197263836.

Volume 2 issue 2

Review by Mark Glover, researcher, UCL Constitution Unit

The photograph on the jacket of this book affords the reader a glimpse through a symbolic glass roof into the innards of the Flemish Parliament. As in the German Reichstag, National Assembly of Wales building and London's City Hall, the glass panes are supposed to represent a transparent 'new politics', which, figuratively as well as literally, "lets the sunshine in". Both the architectural idiom and the political rhetoric are ubiquitous; 'more-transparent-than-thou' is the new 'holier than thou', say the authors, and transparency a new quasi-religion, blessed even by the economic high-priests at the OECD. Therefore, they argue, 'it is vitally important that claims to transparency are tested rather than allowed to go unchallenged'. And from a variety of approaches - including political theory, law, economics, human rights, public administration, and computer science - this is the main contribution of the book.

Their overall tone is interrogative: is transparency a Good Thing? The concept is often blurred with other 'good governance' ideas such as efficiency, accountability, trust, fairness, legitimacy and participation. But which of these are ends and which means? Which are of primary importance and which secondary? And are they all unequivocally and directly linked? Heald explores these issues in chapter 4, 'Transparency as an Instrumental Value'. Transparency is assumed to confer increased knowledge to actors, Heald continues, but can ignorance be useful? Sociologically speaking, as 'a pillar of pre-established social orders', or politically, managing conflict necessitates sending differentiated messages to different parties. Can secrecy be a necessity? It is purported to aid compromise in decision-making bodies, like the EU Council of Ministers, by stopping decision-makers 'pandering' to their constituencies (Stasavage, Chapter 9). When observed, the agent may not act in the 'optimal' way, but according to the wishes of the 'principal', or observer (Prat, Chapter 6).

Doubt is cast on whether transparency measures even achieve their objectives. Where transparency is supposed to improve effectiveness, it can drain resources (Heald, Chapter 4). Where it is supposed to increase trust, it either does not provide enough information for trust-based decisions (O'Neill, Chapter 5), or contributes to a 'rhetoric of secrecy' (Roberts, Chapter 7) and a situation for opponents of government where 'win and you might secure a disobliging revelation about government. Lose and you have a story about official secrecy' (Macdonald, Chapter 8). Instead of nefarious bureaucracy wilting in the sunlight, is it driven into 'ever more secret recesses', as Birkinshaw (Chapter 3) puts it? Roberts describes 'bureaucratic

resistance' to transparency; for example, a failure to create records. This phenomenon has also been described in this journal (Kelly, Vol. 2 Issue 1) and by George W. Bush, 'I don't email (...) and there's a reason: I don't want you reading my personal stuff' (*The Guardian*, 27 October 2006).

The *reductio ad absurdum* then would be support of Official Secrecy, either because of the disbenefits of transparency (the 'jeopardy thesis'), the impossibility of bringing about transparency (the 'futility thesis'), or because transparency achieves the opposite of its objectives (the 'perversity thesis'). These theses are not subscribed to, however. The reader is reminded that Woodrow Wilson and Kant before him believed more openness would lead to fewer wars (Hood, Chapter 1), that politicians use secrecy to avoid taking responsibility for their policy decisions (Stasavage), and that current procedures which effectively turn computer code into law would be better conducted in the open (Camp, Chapter 11).

But lest we forget, McDonald uses freedom of information to remind us of the transparency bottom line: anecdotally at least, people know more. It may almost be a physical battle - for Roberts FOI is 'a tool for regulating the struggle for control of government information'; for McDonald 'it is useful to think of FOI as 'defining the rules of a contact sport. It does not say who will win; but it does rule out certain ploys as illegitimate; and it does give the referee the tools to decide between the competing teams'. As readers – spectators or participants – we are now better informed about the rules of the game.

As a whole, the book successfully unpacks the competing ideas and ideals of transparency. It errs towards 'practical scepticism' and asks more questions than it answers. But in timely fashion, the authors successfully show how light needs to be shed on transparency itself.