CJI/DOC.45/99
RIGHT TO INFORMATION:
ACCESS TO AND PROTECTION OF INFORMATION AND PERSONAL DATA
(presented by Dr. Jonathan T. Fried)

BACKGROUND

The right to information has been on the agenda of the Inter-American Juridical Committee in one form or another since 1980. A comprehensive review of the earlier work of the Juridical Committee was prepared by the previous rapporteur, Dr. Olmedo Sanjur G., and presented in his 1998 report (OEA/Ser.Q CJI/doc.5/98), and thus will not be repeated in this report.

At its twenty-sixth regular session in Panama city in June, 1996, the General Assembly requested the Inter-American Juridical Committee to give special attention to matters concerning access to information and the protection of personal data entered in mail and computerized Committee's deliberations focused on the 1981 Strasbourg Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, and on a possible draft Inter-American convention on self-determination with respect to Information.

At its 53rd regular period of sessions in August, 1998, having reviewed a preliminary draft of an Inter-American Convention in comparison to the Strasbourg Convention, the Juridical Committee recognized that a person's right of access to and protection of personal data raises juridical issues under both domestic and international law. With a view to providing a comprehensive basis for further consideration of the subject, the Juridical Committee therefore requested the Secretariat for Legal Affairs to solicit information from OAS member States on existing domestic legislation, regulations, and policies governing:

a) freedom of, or a person's right to access, information in the possession or control of governments;

b) the protection of personal data against unauthorized use in the possession or control of governments;

c) freedom of, or a person's right to access, information in the possession or control of private entities (for example, utilities, banks or credit agencies);

d) the protection of personal data against unauthorized use in the possession or control of private entities;

e) transborder or international dimensions of the foregoing; and any other domestic legislation, regulations or policies addressing personal data or information in electronic or machine-readable form not otherwise included in [a] through [e] above (OEA/Ser.Q CJI/RES.15/LIII/98).

The General Secretariat requested this information in Note N [OEA/2.2/39/98] on December 8, 1998. Only six member States provided information in response to the request: Costa Rica, Ecuador, Guatemala, Paraguay, Peru and Mexico. This report is based on this information, as well as on research and independent sources of information on Argentina, Brazil, Canada, Chile, Colombia, the

United States and Uruguay. Relevant information concerning other member States was not obtainable prior to the preparation of this report.

This report was prepared with the invaluable assistance of Ms. Laura Belloni (LL.M., University of Ottawa, member of the Argentine bar) and Mr. Daniel Daley, currently Canadian Ambassador to Panama and formerly the Access to Information Coordinator of Canada's Department of Foreign Affairs and International Trade. Any errors or omissions remain the responsibility of the rapporteur alone, however, for which he takes full responsibility.

OVERVIEW

Access to information and protecting personal information and data, are both essential elements of good governance in democratic societies. But they also constitute two sides of the same coin, and must be balanced to ensure respect for individual rights, including the right to privacy.

In democratic societies, it is logical to consider that government information ought to be publicly available wherever possible. In the view of those countries that have adopted access to information or freedom of information regimes, public access to government documents promotes accountability and helps citizens understand how governments make decisions about public policy.

But particularly with the advance of technology, governments generally maintain massive amounts of personal information on their citizens: income tax returns, property tax files, security assessments, social assistance files, immigration and employment records, to name a few. Public access to such records in the name of ensuring freedom of government information may deprive individuals of their ability to protect their privacy.

The objectives of access to information and of protection of personal information are potentially opposed. On the one hand, "access to information" guarantees the inhabitants of a democratic society access to information held by governments, thereby respecting one of the principles of a democratic form of government -- the publicity of the acts of government – and permitting persons to exercise control of these acts through the effective exercise of this right. On the other hand, the protection of personal information and data guarantees the access to one's personal information and at the same time provides for the correction and protection of this information, establishing a shield against public disclosure and preventing access by non-authorized persons.

In a democratic society, the law should protect the privacy of individuals with respect to their personal information held by government institutions and should provide individuals with a right of access to such information. Recognizing that the collection and use of personal information are essential to the administration of many government activities and programs, individuals should nonetheless have the right to a reasonable expectation of privacy, including a basic right to exercise control over their own personal information, a right to know why their information is collected by the government, how it will be used, how long it will be kept and who will have access to it, and a right of access to all of their personal information held by government institutions, subject only to limited and specific exemptions. Viewed in this light, protection of personal information and data is not opposed to principles of accountable government. Public confidence in a government's management of personal information is essential for public trust in, and support of, government programs and actions.

This report therefore analyzes domestic legal regimes on both access to and protection of information in the hemisphere. While a review of available information suggests an ongoing movement towards the enactment of legislation in this field, Canada and the United States have by far the most advanced and well-developed legal regimes, each having been in pace for nearly two decades. On the basis of this North American experience, as well as more recent developments in other member States, this report sets out suggested basic principles on access to information and protection of personal information and data (Part I), highlights various features of domestic legislation in the light of the principles (Part II), discusses the desirability of promoting adherence to the Strasbourg Convention or of developing an inter-American instrument in this field (Part III), provides a preliminary analysis of the challenge of personal information in private hands (Part IV), and makes recommendations in the form of a draft resolution for the consideration of the Juridical Committee.

PART I

BASIC PRINCIPLES

A. Protection of and access to personal information and data

Collection of Personal Information

The collection of personal information plays an essential role in government administration of various programs and activities. Collection of personal data should be prohibited unless it relates directly to a specific government program or activity. Law or policy should require that institutions have administrative controls in place to ensure that they do not collect any more personal information than is necessary for the related programs or activities. This means that institutions must have appropriate legal authority for the relevant program or activity, and a demonstrable need for each piece of personal information collected to carry out the program or activity.

Wherever possible, this information should be collected directly from the person to whom it relates. Collection from other sources should be permitted in cases where the individual is unable to provide the information (for example, an individual who is deceased, incapacitated or who cannot be located despite reasonable efforts) or where direct collection might defeat the purpose or prejudice the use for which the information is collected (as, for example, in criminal investigations) or where information is already in the hands of another government institution authorized to disclose the information, thereby avoiding an unnecessary burden of response by the individual.

Each government institution collecting information should inform an individual of the purpose for which the institution is collecting the individual's personal information. (An exception could be provided for circumstances where informing the individual would result in the collection of inaccurate or misleading information.) This requirement would recognize the individual's right to know and to understand the purpose for which the individual's information is being collected, and how it will be used. In circumstances where the individual is not under an obligation to supply the information, such knowledge and understanding would permit the individual to make an informed decision about whether to respond.

This principle could properly be extended to indirect collections of personal information as well. This would mean that every individual asked to provide personal information (whether the information was about himself or herself or about someone else) would have to be informed of the purpose of the collection, whether response is voluntary or required by law, any possible consequences of refusing

to respond, and that the individual to whom the information pertains has rights of access to and protection of the personal information.

Again, an exception might be made available where so informing the respondent might result in the collection of inaccurate information, or defeat the purpose or prejudice the use for which the information would be collected (for example, where informing the respondent would jeopardize a criminal investigation, or in a survey where informing the respondents of its purpose would jeopardize the validity of the survey results). The application of such an exception could be approved during the collection approval process.

Government institutions should take all reasonable steps to ensure that personal information used for an administrative purpose is as accurate, up-to-date and complete as possible. This requirement would be intended to minimize the possibility that a decision affecting an individual would be made on the basis of inaccurate, obsolete or incomplete information.

Retention and disposal of personal information

Personal information that has been used by a government institution for an administrative purpose should be retained by that government institution for a minimum period of time (for example, two years) following the last use of the information, unless the subject individual consents to its earlier disposal. The law should also require that where a request for access to personal information has been received,2 the institution should retain the information until such time as the individual has had the opportunity to exercise all rights under the law. Similarly, where a request for disclosure of personal information to law enforcement authorities has been made, any information disclosed in response to the request should be retained for a minimum period of time following the date the request was received by the disclosing institution.

There are, inevitably, exceptions to the principle of retention. For example, where an emergency exists at a diplomatic or consular mission abroad, the officer in charge could be authorized to order the destruction of personal information to prevent the removal of the information from the control of the institution. As well, the disposal of personal information prior to the expiration of the minimum retention period could be allowed with the written consent of the individual. This might occur, for example, if the information were determined to be incorrect and if the most appropriate means of correction were disposal, or if the information were no longer required.

Rules for the retention and disposal of personal information by government institutions could properly provide for earlier disposal if the information was collected without respect for the principle of relevant collection and thus is not directly related to an operating program or activity of the institution, where further retention of personal information might unfairly prejudice the interests of the individual to whom the information relates, or where personal information is no longer required for the purpose for which it was obtained or compiled by the institution.

2 See “Right of Access to One's Personal Information", below.

Personal information may, however, have archival or historical value. Procedures should be established to ensure retention and transfer to appropriate archival authorities prior to disposal.

Use of personal information

Consistent with principles of collection, government institutions should use personal information only for the purpose for which the information was obtained or compiled, for uses consistent with that purpose, or for the purposes for which information may be disclosed to them under specific exemption or disclosure provisions.[4]

Disclosure of personal information

Similarly, absent the consent of the subject individual, government institutions should disclose personal information only for the purpose for which the information was obtained or compiled, for uses consistent with that purpose, or for the purposes for which information may be disclosed to them under specific exemption or disclosure provisions.

Governments should require their institutions to have administrative controls in place to ensure that personal information is not disclosed to anyone who is not permitted access under the law.

Consent

Consent should allow government institutions to use or disclose personal information for any purpose consented to by the individual. In other words, the consent of the individual would remove the need to rely on a specific exemption or disclosure provision. Consent by an individual to the use or disclosure of personal information could be sought either at the time of collection of the information or subsequently, when a specific need arises.

If consent for additional use or disclosure is sought at the time that the personal information is collected, government institutions should provide sufficient information concerning the intended use or disclosure to allow the individual to make an informed decision to consent or refuse. Such information should include a description of the specific information involved, the use or disclosure for which consent is being sought, and a statement that refusal to consent to such use or disclosure will not prejudice the individual in any way or result in any adverse consequences for the individual in connection with the primary administrative purpose being served by the information collection.

Consent for use or disclosure subsequent to collection should be obtained in writing. This would normally take the form of a signed consent from the individual or authorized representative, specifying the permitted use or disclosure.

Permissible disclosures of personal information without consent

Privacy demands that government protect personal information and data in its possession or control from disclosure. Various circumstances may, however, demand disclosure without the consent of the individual. Such circumstances should be prescribed by law. Some of the basic grounds for non consensual disclosure include the following:

1. Disclosure for the original purpose and for a consistent use

Personal information may be disclosed for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose. This would give government institutions the discretion to disclose personal information where this is necessary to accomplish the purpose for which the information was obtained or compiled, or for a use consistent with that purpose.

2. Subpoenas, warrants, court orders and rules of procedure of the courts of law

Personal information may be disclosed for the purpose of complying with a subpoena or a warrant issued or an order made by a court of law or a person or a body with jurisdiction to compel the production of information, or for the purpose of complying with the rules of a court relating to the production of information.

3. Disclosure to the chief legal officer of the government for use in legal proceedings

Personal information may be disclosed to the chief legal officer of the government for use in legal proceedings involving the government. This would cover those circumstances where personal information is required by the chief legal officer for the conduct of a case before the courts (or a quasi-judicial body) to which the government is a party or in which it is implicated.

4. Disclosure to government investigative bodies

Personal information may be disclosed to an investigative body specified in the law, on the written request of the body, for the purpose of enforcing any law or carrying out a lawful investigation. The request should specify the purpose for the request and describe the information to be disclosed. Such a provision would not normally grant investigative bodies a right of access to personal information. Rather, it would leave the disclosure decision to the discretion of the institution, once the relevant criteria had been satisfied.

Governments might wish to restrict to senior officials the authority to disclose information under this provision. Moreover, in view of the serious impact that a disclosure under this provision could have on personal privacy, governments might require their institutions to establish internal directives governing the disclosure of personal information pursuant to such a request. These internal directives could distinguish among the various types of personal information (for example, non-sensitive biographical data versus sensitive medical information) and establish guidelines governing the circumstances for disclosure of each type of personal information to investigative bodies.

5. Disclosure to foreign States and international bodies

Personal information may be disclosed under an agreement or arrangement between: 1) the government (or an institution thereof) and 2) the government of a foreign state (or an institution thereof) or an international organization of states (or other similar international organization), for the purpose of administering or enforcing any law or carrying out a lawful investigation.

This provision would accommodate practices whereby personal information is exchanged between police, security and investigative bodies and their international counterparts. Such disclosures aid in effective law enforcement and investigative activities.

6. Disclosure to members of the legislature

Governments may wish to provide that personal information may be disclosed to a member of the legislature for the purpose of assisting the individual to whom the information relates in resolving a problem. Such a provision would be intended for use when a constituent has asked his or her representative in the legislature for assistance, but may not have specifically provided consent for release of his or her personal information. One possible example would be where consular assistance has been sought from the government.

7. Disclosure for audit, archival, research or statistical purposes

Governments would no doubt wish to ensure that the privacy law provides for disclosure of personal information to specified persons or bodies for audit purposes.5 It would be important to provide that personal information may be disclosed pursuant to this provision for audit purposes only and not as part of any decision-making process concerning the individual to whom the information relates.

A provision authorizing disclosure for archival purposes would also be important. "Disclosure for archival purposes" should be defined to include not only the actual transfer of personal information to the control of the national archives for archival and historical purposes, but also the examination by staff of the national archives of personal information held within government institutions to determine whether or not the information qualifies as an archival record and to establish appropriate retention and disposal standards for the information.

Similarly, a provision could authorize a government institution to disclose personal information to any person or body for research or statistical purposes, if the entity is satisfied that the purpose for which the information is to be disclosed cannot reasonably be accomplished unless the information is provided in a form that would identify the individual to whom it relates, and obtains from the person or body a written undertaking that no subsequent disclosure of the information will be made in a form that could reasonably be expected to identify the individual to whom it relates.

8. Disclosure in the public interest

As a supplement to the specific disclosure provisions described above, a government might wish to include in its law an authorization along the following lines: personal information may be disclosed for any purpose where, in the opinion of the head of an institution, (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or (ii) disclosure would clearly benefit the individual to whom the information relates.

This provision would allow the government to deal with situations that either cannot be readily foreseen or are so particular that they cannot suitably be covered in specific terms elsewhere in the provisions authorizing disclosure. The provision would have to be used with a great deal of restraint, and its use would have to be recorded carefully.

Examples of situations in which there could be a public interest that outweighs the potential invasion of privacy in disclosure include:

a) health or medical emergencies, accidents, natural disasters or hostile or terrorist acts where one or more individual's lives and well-being depend on the disclosure;
b) the disclosure of information to carry out an order of a court (for example, the enforcement of a custody order); and
c) the disclosure of information either to substantiate or to correct a statement made publicly by the individual concerned. In these circumstances, the individual would first have made public the information being substantiated or corrected. 9. Disclosure to benefit the individual to whom the information relates

The law should grant to a government institution the discretion to ensure that personal

information is not withheld from disclosure where the individual would clearly benefit from its release. Examples of situations where personal information could be released on these grounds are:

a) disclosure to a doctor or hospital of an individual's blood type in an emergency when a transfusion is needed;
b) notification of next of kin in case of an accident or disaster (or disclosure to an airline of information to locate passengers' next of kin where an accident has occurred); and
c) disclosure of information to assist in determining the owner of lost or stolen property;
d) disclosure of information about an individual to immediate family members or an authorized representative of the individual such as a lawyer, under compassionate circumstances (for example, information as to whether or not an individual has been arrested in another country).

Again, this provision would have to be used with considerable restraint, and its use would have to be accounted for.

Right of access to one's personal information

An individual's right of access to government-held information about him or herself, within a specified time limit, is an essential element of accountable government, as noted above. Access to one's own personal information may, however, be subject to broader public interests. Following are examples of exemptions often found in privacy laws:

1. Cabinet confidences

In a cabinet system of government, confidences of the cabinet6 are generally outside the application of the privacy law. The exclusion of such information is considered necessary for the preservation of the confidentiality of deliberations essential to the effective functioning of this system of government.

2. Information received in confidence

The privacy law would normally provide that a government institution shall refuse to disclose any personal information that was obtained in confidence7 from the government of a foreign state or an institution thereof, or an international organization of states or an institution thereof. The government institution should, however, be given the discretion to disclose personal information obtained in confidence from another government or an international organization if the government or organization from which the information was obtained consents to the disclosure or makes the information public.

Cabinet confidences would generally include: documents that present proposals or recommendations to the cabinet; agenda of cabinet or records recording deliberations or decisions of cabinet; records of communications or discussions between cabinet ministers on matters relating to the making of government decisions or the formulation of government policy; documents to brief ministers in relation to cabinet business; and draft legislation.

In this context, the term "in confidence" means that the supplier of the information does not wish it to be disseminated

beyond the institution to which it has been supplied. Wherever feasible, it is advisable that government institutions enter into agreements with those other governments, international organizations or their institutions with which they will be exchanging information, stipulating the information that is being exchanged in confidence.

3. International affairs and defence

Governments would, no doubt, wish to include in law provision to permit a government institution to refuse to disclose any personal information the disclosure of which could reasonably be expected to be injurious to the conduct of international affairs, the defence of the state or any state allied or associated with the state, or the detection, prevention or suppression of subversive or hostile activities.

To prevent the exemption from being used to circumvent the privacy law or otherwise to undermine its effectiveness, the government would doubtless wish to ensure (as with the other exceptions to the disciplines of the privacy law) that there are effective provisions for the review by an independent body (preferably a court of law) of decisions by government institutions to invoke this exemption, as discussed below.

4. Law enforcement, investigations and penal institutions

As with international affairs and defence, governments may wish to ensure that the law gives discretion to a government institution to refuse to provide access to personal information to the extent necessary for effective law enforcement, including criminal law enforcement, the integrity and effectiveness of other types of investigative activities (for example, investigations in regulatory areas and air accident investigations), or the security of penal institutions.

5. Safety of individuals

A government institution may refuse to disclose any personal information the disclosure of which could reasonably be expected to threaten the safety of individuals. This exemption would normally apply to information by or about informants. It could include individuals who provide information concerning criminal, subversive or hostile activities, but it would not necessarily be limited to such individuals.

6. Information about another individual

Privacy law embodies the principle that an individual has a right of access only to information about himself or herself. This principle is clearly applicable where personal information about one individual is combined inseparably with information about another individual (for example, information about a husband and wife in an immigration file). When this occurs, such information should not be disclosed unless some discretion to disclose the information is specifically granted in the law.

7. Lawyer-client privilege

Communications between lawyer and client are treated as privileged in virtually all jurisdictions. Consistent with the special status accorded to these communications, the law should provide that a government institution may refuse to disclose any personal information that is subject

to lawyer-client privilege. This provision would normally allow the government institution to claim the

8 To avoid overly-broad interpretations or abuse of such exemptions, "subversive or hostile activities" could be defined as:
a) espionage against the state or any state allied with or associated with the state; b) sabotage; c) activities directed toward the commission of terrorist acts, including hijacking, in or against the state or foreign states; d) activities directed toward accomplishing government change within the state or foreign states by the use of or encouragement of the use of force, violence or any criminal means; e) activities directed toward gathering information used for intelligence purposes that relates to the state or any state allied with or associated with the state; and f) activities directed toward threatening the safety of nationals of the state, employees of the government of the state or property of the government of the state outside the state.

The exemption would be intended to be used when the disclosure of information could circumvent the normal procedures (such as the process of "discovery") in cases before the courts, prejudice the government's legal position in present or future litigation or negotiations, or impair the ability of government institutions to communicate fully and frankly with their legal advisers. Corrections and notations

As a basic complement to an individual's right of access to his or her personal information that is held by a government institution, every individual should protect the right of an individual to ensure the accuracy of the information gathered and to request correction of the information where there is an error or omission. Accordingly, where a correction is accepted by the government institution, the institution should, within a specified time, notify both the individual and any person or body to whom the information has been disclosed.

Where a request for correction is refused in whole or in part, the government institution should, within a specified time, attach a notation to the personal information reflecting that a correction was requested but was refused in whole or in part, notify the individual that the request for correction has been refused in whole or in part and give the reasons for the refusal, and notify any person or body to whom the personal information was disclosed that the request for correction was received and that a notation has been attached to the personal information.

The corrections and notations should be stored in a manner that will ensure that they are retrieved and used whenever the original personal information is used for an administrative purpose.

Independent review of decisions

For the effective administration of law for the protection of personal information and data, there should be an independent review available with respect to decisions taken under the law. This would mean that, at a minimum, an ombudsperson who is independent of the government should be empowered to review the following matters, at the instance of the affected individuals:

- the use or disclosure of personal information otherwise than in accordance with the privacy law;
- the denial of a request by an individual for access to his or her personal information;
- the failure by an institution to accord rights relating to the correction or notation of personal information, or to notify other institutions of such corrections or notations;

- the extension of time limits for response to a request for access to one's personal information; and
- any other matter relating to the collection, retention and disposal; use or disclosure; or requesting or obtaining access to personal information under the control of government institutions.

Judicial review

Governments should also consider establishing a right of appeal to the courts (either by the affected individual or by the ombudsperson), at least with respect to the denial by a government institution of a request for access to one's personal information.

B. Access to information held by governments

As noted in the Overview, citizens should have the right of access to information held by their government. While it may be argued that this access should be guaranteed to any person, requiring certain conditions pertaining to citizenship or permanent residency may be considered as justified on the basis of to whom governments are accountable.

Access should be guaranteed for all the information held by governments, including information under the possession or control of government. Public access should not be frustrated except under clear grounds, so that in case of doubt as to disclosure of information, it would be resolved in favour of disclosure. Therefore, the right of access should be the rule, and the exceptions to this principle should be specific and limited to certain circumstances. The law should also establish the definition what is to be considered a government institution, such as the federal government, departments, or agencies. The trend is to extend coverage of access to all the organizations that deliver public services or fulfill statutory functions even where these organizations are private institutions.

Exemptions to the right of access to information

As suggested above, the basic principle of access to information should be disclosure. Exceptions to this right should be limited and specific. Some circumstances demand automatic denial of disclosure, for example in respect of personal information or commercially confidential information, such as trade secrets or other third-party information. Other circumstances may require a determination of a risk or harm or injury that might be provoked by the disclosure, such as possible effect on the conduct of international affairs.

Independent review of decisions on disclosure

As is the case for decisions respecting personal information or data, where the government institution to which a request for disclosure of information is made refuses access, the individual should have the right to order the revision of this decision before an independent body. Here, disclosure may not only be expressly denied but also implicitly denied where the government institution is silent or takes an unreasonable amount of time in responding to an individual's request. In these cases, an independent office or ombudsperson should be authorized to review these decisions or situations.

This office could play the role of mediator prior to judicial review to bring the government institution and the individual to an arrangement or understanding. The office could also usefully be authorized to self-initiate reviews. The office may or may not have the power to enforce decisions, but should at a minimum be give authority to make a recommendation to the government institution to proceed with disclosure.

Judicial review

Where the independent office does not recommend disclosure or having recommended disclosure the government institution does not follow the independent body's recommendations, the requester should be authorized to seek judicial review of the administrative action (or inaction). Judicial review of decisions should be authorized especially in cases where no independent administrative review is available or provided.

As mentioned above, accountability demands a presumption in favour of disclosure, so the burden of proof should rest on the party resisting disclosure, whether it be the government, corporation or individual. Where an independent office is established by law, the latter should be able to present itself as a party before the court, whether it supports disclosure or denial of disclosure.

The court should be empowered to order disclosure.

Third party procedures

Where the information that is to be disclosed pertains to a third party, that party's right to resist disclosure should be guaranteed by law. Such procedures are generally available for the protection of business information and not for personal information, which is considered to be confidential. However, as in the case of government institutions, the burden of proof with regard to

the decision to disclose or not should rest with the third party that resists disclosure.

Procedure to access to information

The right of access to information held by government institutions should be guaranteed by procedures, thereby respecting the principle of due process. These procedures should be initiated by written application by the individual interested in the disclosure of information. This written application may take several forms. The government institution should be granted a limited period of

time (days) to respond to the request for information, subject to exceptional circumstances provided by law. Moreover, where third party information is to be released, the government institution should give notice to this party in order to allow him or her to demonstrate why the information should not be disclosed. The government institution that refuses to disclose the information should always cite the statutory ground for its refusal.