CJI/doc.25/00 rev.2
RIGHT TO INFORMATION:
ACCESS TO AND PROTECTION OF INFORMATION
AND PERSONAL DATA IN ELECTRONIC FORM
(Updated by the Office of International Law of the
Department of International Legal Affairs of the report
submitted by Dr. Jonathan T. Fried at the 57th regular session
of the Inter-American Juridical Committee, CJI/doc.25/00 rev.1)

INTRODUCTION

1. Background

At its twenty-sixth regular session in Panama City in June 1996, the General Assembly requested that the Inter-American Juridical Committee pay special attention to matters concerning access to information and the protection of personal data entered in mail and computerized electronic transmission systems [AG/RES. 1395 (XXVI-O/96)]. The Inter-American Juridical Committee concluded an analysis (OEA/Ser.Q CJI/doc. 52/98) of the Convention for the protection of individuals with regard to automatic processing of personal data or Strasbourg Convention relating to a draft American Convention on self-determination with respect to information.

At its fifty-third meeting in August 1998, the Juridical Committee asked the Secretariat for Legal Affairs to solicit information from OAS member States on existing domestic legislation, regulations and policies concerning:

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

f) 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.[12]

The General Secretariat requested this information in Note N OEA/2.2/39/98 on 8 December 1998. Six member States provided information in response to the request: Costa Rica, Ecuador, Guatemala, Paraguay, Peru and Mexico. Based on the information submitted, as well as independent research, a report entitled “Right to information: access to and protection of information and personal data” (OEA/Ser.Q CJI/doc.45/99) was tabled by the rapporteur to the Inter-American Juridical Committee of the OAS in August 1999. The focus of that report was governmental regulation of personal information and data held in government hands. In its resolution (CJI/RES.9/LV/99), the Juridical Committee requested the General Secretariat to reiterate its request for information from Member States; this was done through process-verbal OEA/2.2/32/99. At the 57th regular session of the Inter-American Juridical Committee, doctor Jonathan Fried, submitted document CJI/doc.25/00 rev.

1, "Right to information: access to and protection of information and personal data in electronic format", which is further described in the following section.

The Inter-American Juridical Committee requested the Secretariat of Legal Affairs through Resolution CJI/RES.13 (LVII-O/00) to present the two reports on the subject prepared by the rapporteur for the information of the States and reiterate its prompt request for information from member States.

At the 63rd regular session of the Inter-American Juridical Committee (Rio de Janeiro, August, 2003), doctor Alonso Gómez-Robledo suggested the inclusion of the subject relating to access to public government information in the Committee's agenda. The members of the Juridical Committee agreed to include this matter as follow-up under the same title with which the right to information previously appeared in the agenda, that is, "Right to Information: Access to and protection of information and personal data".

The General Assembly, at its 34th regular session (Quito, June, 2004), through resolution AG/RES. 2042 (XXXIV-O/04), noted the importance of including this topic in the agenda of the Inter-American Juridical Committee and requested the inclusion of an updated report on this matter in its next annual report.

At its 65th regular session (Rio de Janeiro, August, 2004), the Inter-American Juridical Committee examined document CJI/doc.162/04, "Right to information: access to and protection of information and personal data", submitted by doctor Alonso Gómez Robledo. The rapporteur on this matter outlined in such report the interdependence between accountability and transparency in the exercise of democracy.

The General Assembly, at its 35th regular session (Fort Lauderdale, June, 2005), through resolution AG/RES. 2069 (XXXV-O/05) "Observations and recommendations to the Annual Report of the Inter-American Juridical Committee", noted the importance of the topic and requested the Committee to include in its annual report an updated report on the protection of personal data based on compared legislation.

The General Assembly of the OAS at its 36th regular session (Santo Domingo, June, 2006), through resolutions AG/RES. 2218 (XXXVI-O/06) and AG/RES. 2252 (XXXVI-O/06), requested the Inter-American Juridical Committee the inclusion in its next annual report of an updated report on the protection of personal data based on compared legislation. It also requested the Committee to make an update of the study "Right to information: access to and protection of information and personal data in electronic format" of the year 2000 taking into account the various viewpoints on the issue, and to this end will prepare and distribute a new questionnaire on the topic among the member States, with the Secretariat's support.

[12] OEA/Ser.Q CJI/RES.15/LIII/98.

At its 69th regular session (Rio de Janeiro, August 2006), and concerning resolutions AG/RES. 2218 and AG/RES. 2252, the three specific tasks entrusted to the Committee were recapped: 1) include in its annual report an updated report on the topic of protection of personal data based on compared legislation; 2) update the specific study of the Juridical Committee carried out in the year 2000; and 3) prepare and distribute a new questionnaire on the topic for OAS member States.

During the same period, the President reminded the Juridical Committee about the report prepared by doctor Jonathan Fried on the matter of the protection of personal data and requested the General

Secretariat an update of such study based on compared legislation to be submitted not later than November 15, 2006. The "Questionnaire for OAS Member States Regarding the Legislation on Access to and Protection of Personal Data in View of the Preparation of a Juridical Document", document CJI/doc.232/06 rev.1, of August 17, 2006, was also discussed. After its consideration, the Juridical Committee approved the document and requested its circulation among the OAS member States for the subsequent preparation of the study of the Juridical Committee regarding this issue.

2. Report of Rapporteur Jonathan Fried

As it was previously stated, based on part of the questionnaires referred in the preceding paragraph, the Inter-American Juridical Committee through its rapporteur, doctor Jonathan Fried, submitted at the 57th regular session of the Inter-American Juridical Committee, report CJI/doc.25/00 rev.1, which addresses the regulation through international instruments as well as at the level of the legislation of some OAS member countries, of the processing of personal data by the private sector. This report was prepared with the assistance of and based on in-depth research carried out by Thomas Fetz, Counsel of the Bureau of Legal Affairs of Canada's Department of Foreign Affairs and International Trade.

This report is a valuable input not only to understand the true dimension of this issue in the light of the impact that new technologies have on the expansion of the manipulation and use of the information by individuals, but to help States to take actions regarding law harmonization, improved regional cooperation and finding substantial elements for a future regional instrument on the matter. The report examines the regulatory norm inherent to the protection of and access to personal data held in electronic format by private organizations. While data protection in the private sector can be improved using various means, even the market forces, technology, and self-regulation,13 the focus of this report will be on governmental regulation.

With advances in computer technology medicine and biotechnology, there has been a marked increase in the processing of personal data in the various spheres of economic and social activity. The progress made in information technology also makes the processing and exchange of such data across international borders relatively easy. The challenge, therefore, is to protect fundamental rights and freedoms, notably the right to privacy and the right to access personal information (also known as *habeas data*), while encouraging the flow of information and electronic commerce.

3. Update

In the Special Session of the Commission on Juridical and Political Matters conducive to promote, disseminate and exchange experiences and knowledge relative to access to public information held on April 28, 2006, in Washington, D.C., the Rapporteur of the Inter- American Committee on the matter of access to information, doctor Jaime Aparicio, made a presentation which updated doctor Fried's report. In his presentation, Dr. Aparicio stated that the mandates that he has received from the Inter-American Juridical Committee regarding the issue of access to information have been limited to just one aspect of this broad issue which is access to and protection of personal information of individuals. This information includes, among others, medical records, study records, credit history, judicial records, employment background, financial records, personal files in public and private entities, applications, etc.

13 The protection of personal data can be achieved through instruments such as consumer contracts, privacy policies and codes of conduct. For example, the International Chamber of Commerce has published a proposed model contract for transborder flows of personal data (online: <http://www.iccwbo.org>). Information on model policies, agreements and codes of conduct can be obtained from Privacy Exchange (online: <http://www.PrivacyExchange.org>).

The technological advances, the Internet and other means of information transmission have increased the risk of personal privacy and the right to control, protect and prevent the dissemination of personal information. The legal protection of privacy in this new reality is still precarious.

The laws and regulations on privacy initially only referred to the public sector since only the Governments held personal information on the individuals. However, the current use of personal information is not only a phenomenon between the State and the citizen but also a topic that increasingly involves the private sector and commercial businesses which collect and use personal information for commercial purposes, and in view of the nature of these operations, the information also crosses State borders and becomes an international phenomenon.

The information update submitted by doctor Aparicio was based on research in coordination with the OAS Secretariat with the collaboration of the Office of International Law, which allowed the collection of information on new laws and projects relative to the matter and added information on some countries that were not included in the previous report. However, it was considered that this information should be requested again through the OAS Department of International Juridical Matters to all member States in order to have specific and accurate information regarding the legal progress in the protection of information in the Americas.

In any case, and it does not imply that these are the only countries which have made progress in the matter, we have information from the following countries: Argentina, Brazil, Chile, Canada, Mexico, United States, Peru, Uruguay, Colombia, Paraguay, Ecuador, Costa Rica, Panama and Venezuela.

Taking into account the background that has been mentioned so far, the present update report intends to incorporate doctor Fried's report to the update presented by doctor Jaime Aparicio, including the changes occurred in the aforesaid countries in addition to providing data regarding other counties, apart from the convenience of requesting updated information from the countries. This information can contribute to the initiative to have a regional legal framework that would contribute to regulate the access to and protection of information.

The present document is divided into three parts. The first one discusses the regulation of data processing in the private sector by means of international instruments as well as legislation by a number of OAS countries. The second part explains how these international agreements and national laws address the issue of privacy protection in the context of transborder flows of personal data. Finally, the report identifies various approaches available for the regulation of the international flow of personal data, ranging from the international harmonization of data protection laws to the development of mutual assistance treaties.

I. REGULATION OF DATA PROTECTION IN THE PRIVATE SECTOR

1. Background

Laws and regulations concerning access to and protection of personal data have initially focused on the public sector. This was the case because governments generally hold a great deal of information about individuals. Yet, private organizations are making increasing use of sensitive information and personal data as governments have been offloading services to the private sector and as new opportunities in electronic commerce emerge. Improvements in technology, particularly in the area of computers and telecommunications, have vastly expanded the possibilities of collecting, storing, accessing, and comparing personal information. With the expansion computer networks and particularly the Internet, information can be made available to thousands, if not millions of users,

simultaneously and worldwide.14 Currently more than 150 million people use the Internet and that number is expected to grow to about 510 million by 2003. In 1998, the Internet created revenues of US$301 billion and this figure is expected to multiply over the next few years.[15]

[14] The Internet dates back to 1968 when the contract for its development was awarded. The physical internet was built a year later. The World Wide Web was introduced in 1992. Michael Power, "Bill C-6: Federal Legislation in the Age of the Internet" Manitoba Law Journal (1999) 26(2): 235.
[15] OAS. Department of International Law. *Privacy, access to information and the internet in the European Union, the United States and Latin America: a comparative study*. SG/SLA DDI/doc.01/00. Washington, D.C.: General Secretariat, Feb.2, 2000. p. 3.

Because personal information can be useful for marketing and sales, private organizations increasingly seek such information from individuals by traditional means or on the Internet.16 Individuals often disclose personal data voluntarily on the Internet when visiting commercial sites, registering with discussion groups, entering contests, or voicing their opinions. The type of information disclosed may concern a person's name, civic and email addresses, telephone numbers, occupation, income, marital status, age, sex, or credit card details. In addition, users of digital technologies often produce "electronic footprints", that is, digital information about where they have been, what they were looking at, the messages they sent, and the goods and services they bought. For example, "surfing" on the Internet leaves behind certain "header information" which may reveal:

a) the Internet Protocol (IP) address containing the domain name and the name and location of the organization who registered the domain name;

b) information about the user's operating system and hardware platform;

c) the time and date of the visit;

d) the Uniform Resource Locator (URL) of the Web page which was previously viewed;

e) the query put into a search engine if applicable, or

f) the user's e-mail address if it is in the browser's preference configuration screen.

Furthermore, when browsing through a web site, a user can leave behind "click-stream data" which provide information on the pages visited, the time spent looking at a page and the information sent and received. This information gathering about users may be facilitated by the use of "cookies" which are small data packets sent from the web site server to the user's hard drive. These cookies assign a unique code to each visitor and may be accessed by the server when the user subsequently visits the web site. Some cookies permit the user to gain quicker access to a web site, but can also be used to track a user's movements on the web. This type of technology, while it has its advantages, increases the risk of automatic data collection, use and disclosure without a person's knowledge or consent.[17]

As in the public sector, personal data held in the private sector may be subject to unauthorized collection, use, or disclosure, either deliberately or accidentally, and measures to minimize such activities have to be taken. Yet, the regulation of the protection of and access to personal data needs to be sensitive to the needs of data subjects, including users and consumers as well as businesses and other organizations. These needs are not necessarily contradictory. For example, confidence in on-line privacy protection is an essential feature for the growth of electronic commerce.18 Consumers are concerned about their right to privacy in an increasingly interconnected electronic environment, and businesses want to reassure consumers and avoid interruptions in transborder data flows.

Essentially, data protection is a question of striking the right balance between the rights of individuals to have their personal data protected and the free flow of information. Yet, as on many

other issues, States may not agree on where the proper balance should be or whether data protection is more a human rights issue or an economic issue.

2. International Instruments

Some efforts have been made at the international level to establish common principles for the protection of personal data in the private sector. While the direct effect of international instruments varies, several of them have clearly influenced national laws and self-regulatory mechanisms on privacy protection.

a) International human rights instruments

The right to privacy is enshrined in several international human rights instruments.[19] Article 12 of the Universal Declaration of Human Rights[20] states the following:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Article 17 of the International covenant on civil and political rights[21] uses almost identical terms:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

The American Convention on Human Rights[22] provides for the express protection of "private life" in Article 11:

1. Everyone has the right to have his honor respected and his dignity recognized.
2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.
3. Everyone has the right to the protection of the law against such interference or attacks.

Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[23] guarantees the right to privacy and secrecy of correspondence:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[16] Collecting personal information about individuals and their preferences to target consumers is referred to as "data mining" and considered an invasion of privacy by many.

[17] Organization for Economic Cooperation and Development; Directorate for Science, Technology, and Industry; Committee for Information, Computer and Communications Policy; Working Party on Information Security and Privacy; "Inventory of Instruments and Mechanisms Contributing to the Implementation and Enforcement of the OECD Privacy Guidelines on Global Networks" DSTI/ICCP/REG (98) 12/FINAL, (19 May 1999) p. 7-8.

[18] The growth of electronic commerce also raises a host of other questions with respect to consumer protection. The Organization for Economic Cooperation and Development has recently issued its "Recommendation of the OECD Council Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce" (19 Dec. 1999). Online: OECD: <http://www.oecd.org/dsti/sti/it/>.

The principles expressed in these human rights instruments are often referred to in treaties or conventions dealing specifically with the protection of personal data.

b) OECD Guidelines

On 23 September 1980, the Council of the Organisation for Economic Cooperation and Development (OECD) adopted the Recommendation concerning guidelines governing the protection of privacy and transborder flows of personal data[24] (OECD Guidelines) which provides minimum standards for the protection of personal data. While the OECD Guidelines are not binding under international law, they represent a political commitment by the member States. The OECD Guidelines cover "any information relating to an identified or identifiable individual" and apply data processing in the public and private sector.[25]

The OECD Guidelines recommend that "Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines" and that they "endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data". The principles outlined in the OECD Guidelines are as follows:

[19] See: Lee A. Bygrave, "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties" International Journal of Law and Information Technology (1998) 6(3): 247.
[20] Online: United Nations High Commissioner for Human Rights, Treaties: <http://www.unhchr.ch/udhr/lang/eng.htm>.
[21] Online: United Nations High Commissioner for Human Rights, Treaties: <http://www.unhchr.ch/html/menu3/b/a_ccpr.htm>.
[22] Online: Organisation of American States, Treaties and Conventions: <http://www.oas.org/>.
[23] E.T.S. 5, signed 11 Apr. 1950, entered into force 3 Sept. 1953; online: Council of Europe, Treaty Office, <http://conventions.coe.int/treaty/EN/cadreprincipal.htm>.
[24] OECD Document C(80)58/FINAL (1 October 1980); online: OECD: <http://www.oecd.org/dsti/sti/it/secur/prod/priv-en.htm> [hereinafter: OECD Guidelines].
[25] OECD Guidelines, Part One.

Collection limitation
Data should be obtained by lawful and fair means and with the knowledge and consent of the data subject where appropriate.

Data quality
Personal data should be relevant to the purposes for which they are used and accurate, complete, and up-to-date.

Purpose specification
Personal data should be collected and used only for specified purposes.

Use limitation
The use or disclosure of personal data should be limited to the purposes specified, unless provided otherwise by law or consent of the data subject.

Security safeguards
Reasonable security safeguards should be put in place against risks such as loss, unauthorized access, destruction, use, modification or disclosure of personal data.

Openness
Policies and practices with respect to personal data should be open and transparent.

Individual participation
Data subjects should have the right to access their personal data and to have them corrected or destroyed in a manner that is reasonably understandable and cost and time efficient.

Accountability principle
Data controllers should be held accountable for complying with the measures set out in the Guidelines.[26]

The OECD Guidelines recommend that countries implement these principles by: a) adopting appropriate legislation; b) encouraging self-regulation; c) providing reasonable means to individuals to exercise their rights; d) providing adequate sanctions and remedies where there is a lack of compliance; e) and ensuring that there is no unfair discrimination against data subjects.[27] The fundamental weakness of the OECD Guidelines, however, is their voluntary nature.

c) Council of Europe Convention

Unlike the OECD Guidelines, the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data[28] is a binding international

legal instrument. The Convention was adopted on 18 September 1980, opened for signature on 28 January 1981, and entered into force on 1 October 1985 after five ratifications. Any State, even those which are not members of the Council of Europe, may accede to the Convention. The Convention is applicable to the automated processing of personal data in the public and private sectors.[29]

The Convention obligates States to incorporate certain principles regarding the collection and processing of personal data into their domestic law. These principles are similar to those of the OECD Guidelines. Article 6 of the Convention, however, adds a further principle providing for appropriate safeguards for data revealing information about racial origin, political opinions or religious and other beliefs, health or sexual life, or criminal convictions. Member States are also required to establish "appropriate sanctions and remedies for violations of domestic law giving effect to the basic principles".

The Council of Europe Convention has provided an important impetus for member States to enact laws regulating the flow of personal data. On its own it is not a very strong instrument for the protection of personal data given that its interpretation and implementation rests with the national authorities of the member States.

II

[26] OECD Guidelines, Part Two.

[27] OECD Guidelines, Part Four.

[28] European Treaty Series No. 108; Council of Europe, Treaty Office: <http://conventions.coe.int/treaty/EN/cadreprincipal.htm> [hereinafter Council of Europe Convention].

[29] States are, however, permitted to limit the scope and application of the Convention by a declaration addressed to the Secretary General of the Council of Europe. Council of Europe Convention, Article 3.

The Consultative Committee established under Article 18 of the Convention has recently drafted an "Additional Protocol"[30] dealing with the establishment of supervisory authorities and transborder data flows. This draft Protocol would require Parties to establish independent supervisory authorities which ensure compliance with domestic laws giving effect to the principles set out in the Convention. These supervisory authorities (privacy commissioners or data protection officers) would hear complaints about violations of privacy laws and would have the power to investigate and intervene, as well as to engage in legal proceedings where privacy provisions of domestic laws are violated.[31]

The Council of Europe also encourages self-regulation through codes of conduct with respect to the processing of personal data. For example, the Committee of Ministers recommended to member States the dissemination of the Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways which are addressed directly to internet service providers and users.[32]

d) United Nations Guidelines

The United Nations General Assembly adopted the United Nations High Commissioner for Human Rights' Guidelines for the regulation of computerized personal data files (UN Guidelines),[33] pursuant to Article 10 of the United Nations Charter, in 1990.[34] The UN Guidelines, which are non-binding, provide minimum standards for States to adopt when regulating privacy protection for public and private computerized and manual files.[35]

The principles included in the UN Guidelines are lawfulness and fairness, accuracy, purpose-specification, access, non-discrimination, power to make exceptions (national security, public order, public health and morality, and rights and freedoms of others), security, as well as supervision and sanctions. These principles are similar to those of the OECD Guidelines. Additional protection is provided through the prohibition of the compilation of *"data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union."*[36]

The UN Guidelines call upon countries to designate independent, impartial and technically competent authorities responsible for overseeing the principles set out in the Guidelines. Sanctions for violations of the principles should include appropriate criminal or other penalties as well as individual remedies.[37]

e) European Union Privacy Directive

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of individuals with regard to the processing of personal data and on the free movement of such data[38] (EU Directive) was signed in 1995 and was to be implemented by the Member States by 24 October 1998. It requires Member States to have laws in place

establishing a minimum level of protection regarding the processing of personal data by whatever means. States are free to pass laws with stricter standards than those set by the EU Directive. The EU Directive recognizes that "personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded." The EU Directive applies to the processing of personal data by any person whose activities are governed by Community law, in the public and private sectors, but not to

II

30 Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, "Draft Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108) regarding supervisory authorities and transborder data flows," Strasbourg, 8 June 2000; web site of the Council of Europe, Personal Data Protection: <http://www.coe.fr/dataprotection/Treaties/projet%20de%20protocole%20E.htm> [hereinafter Draft Protocol].

31 Draft Protocol, Article 1.

32 Recommendation No.R (99) 5 of the Committee of Ministers to Member States for the Protection of Privacy on the Internet: Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways (adopted by the Committee of Ministers on 23 February 1999 at the 660th meeting of the Ministers' Deputies) at the web site of the Council of Europe, Personal Data Protection: <http://www.coe.fr/dataprotection/rec/elignes.htm>.

33 United Nations High Commissioner for Human Rights: <http://www.unhchr.ch/html/menu3/b/71.htm>.

34 Resolution 45/95, 14 December 1990, at the web site of the United Nations, Documentation Centre: <http://www.un.org/gopher-data/ga/recs/45/95>.

35 The UN Guidelines also apply to personal data files kept by governmental international Organizations.

36 UN Guidelines, Article 5.

37 UN Guidelines, Article 8.

38 Directive 95/46/EC, 24 October 1995, Official Journal of the European Communities, L 281 (23 November 1995), at 31. The text of the European Union Privacy Directive can also be found at: Eur-Lex: <http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html> [hereinafter EU Directive].

processing operations concerning public security, defence, State security, and State activities in the areas of criminal law. Neither does it apply to the data processing activities of natural persons in the course of a purely personal or household activity.[39]

The privacy protection principles set out in the EU Directive are broader and more detailed than those of the OECD Guidelines. Data can only be processed if the "data subject" has given "unambiguous consent".[40] Such consent must be explicit with respect to "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[41] Even where consent has been obtained to process information, the data subject must "be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses."[42]

Generally, processing without consent can proceed only if one of five exceptions applies. The processing is 1) "necessary for the performance of a contract to which the data subject is party"; 2) "necessary for compliance with a legal obligation"; 3) "necessary in order to protect the vital interests of the data subject"; 4) "in the public interest"; or 5) "processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection."[43]

The data subject must be informed about the identity of the controller (the person determining the purpose and means of processing data); the purpose of the data processing, and about any other relevant information to "guarantee fair processing". Data subjects also have a right to access and to correct or erase personal data. Data subjects are enabled to monitor and challenge the use of personal information during and after processing. They can trace which third parties hold their personal information, verify how they are using it, and block unauthorized uses.[44] Furthermore, they have a right to challenge ("not to be subject to") any decision which significantly affects them, such as one that is based on an automated processing of data intended to evaluate personal aspects such as performance at work, creditworthiness, reliability, conduct, etc."[45]

The member States of the EU are responsible for the implementation as well as enforcement of the EU Directive. States must guarantee data subjects the right to a judicial remedy, and wronged data subjects must be able to obtain damages.[46] The implementation of the EU Directive's principles on privacy protection is to be reinforced by a supervisory authority. These authorities must "act with complete independence" and have "investigative powers" which allow them access to data and to collect information. In addition, they must

have “effective powers of intervention” such as the ability to deliver opinions, to publicize matters, or to order the blocking or destruction of data. The supervisory authorities must also have the power to engage in legal proceedings or to bring matters to the attention of judicial authorities.[47]

f) General agreement on trade in services

Given the impact trade rules have on so many aspects of economic and social activity, reference should be made to the *General agreement on trade in services* (GATS)[48], which is part of the World Trade Organization (WTO) treaty framework. Article XIV of the GATS states:

Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where

[39] EU Directive, Article 13.
[40] EU Directive, Article 7.
[41] EU Directive, Article 8.
[42] EU Directive, Article 14. Direct marketing sales in Europe totalled 125 billion dollars in Europe in 1997, compared to 1.2 trillion dollars in the United States. Gregory Shaffer, “Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards,” (2000) 25(1) Yale Journal of International Law 1 at 18.
[43] EU Directive, Article 7.
[44] EU Directive, Articles 10, 11 & 12.
[45] EU Directive, Article 15.
[46] EU Directive Articles 22-24.
[47] EU Directive, Article 28.
[48] Web site of the World Trade Organization, Legal Texts: <http://www.wto.org/english/docs_e/legal_e/final_e.htm> [hereinafter GATS].

like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any member of measures:

c) (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.[49]

Thus, while the GATS prohibits discrimination and disguised trade barriers, there is room for national authorities to regulate the transborder flow of data for purposes of privacy protection.

3. National legislation

At the national level, data protection in private sector organizations has taken the form of constitutional protections, comprehensive laws, sectoral laws, self-regulation, or a combination thereof. Comprehensive laws tend to apply general privacy protection principles to a wide range of sectors, both public and private. Sectoral laws are concerned only with specific sectors, such as communications, or with specific data such as medical information. Most countries’ laws include general data protection principles, provisions for oversight authorities, generally known as privacy commissioners or data protection officers, and some reference to industry self-regulation. The roles and powers of oversight authorities usually concern public education, the investigation of complaints, and enforcement. Self-regulation relies on market forces and industry-led initiatives to provide innovative solutions. The rules are developed and enforced by those to whom they apply. In some cases, however, independent bodies or public entities are involved in the development, implementation and enforcement of industry codes and guidelines.

Data protection in Latin America is strongly tied to the concept of *habeas data* which guarantees individuals a right to access their personal information. It is based on the recognition that an individual should have control over the data gathered about him or herself. The principle emerged recently in response to the detrimental impact of the use of computers on privacy rights. The Brazilian Constitution of 1988 was the first to use the expression *habeas data*. Thereafter, the right of individuals to access their personal information was included in the national constitutions of several other Latin American States, including Argentina, Colombia, Paraguay, Peru and Venezuela.[50]

a) Argentina

1) ARGENTINE CONSTITUTION

The 1994 Constitution of Argentina provides some protection for privacy. Article 18 states:

The domicile may not be violated, as well as written correspondence and private papers; and a law shall determine in which cases and for what reasons their search and occupation shall be allowed.
Article 43 of the Constitution provides for the right of *habeas data* as follows:
1. Any person shall file a prompt and summary proceeding regarding constitutional guarantees, provided there is no other legal remedy, against any act or omission of the public authorities or individuals which currently or imminently may damage, limit, modify or threaten rights and guarantees recognized by this Constitution, treaties or laws, with open arbitrariness or illegality. In such case, the judge may declare that the act or omission is based on an unconstitutional rule.
....
3. Any person shall file this action (1) to obtain information on the data about himself and their purpose, registered in public records or data bases, or in private ones intended to supply information; and in case of false data or discrimination, this action may be filed to request the suppression, rectification, confidentiality or updating of said data.

II

[49] GATS, Article XIV c(ii).
[50] OAS. *Op.cit*., p.26.

2) LEGISLATION

In 1996, legislation giving effect to the provisions of Article 43 of the 1994 Constitution was approved by the Senate and the Chamber of Deputies.[51] This statute was vetoed by President Menem following interventions by the Banking Association, who considered that the disclosure and privacy provisions were too strong, and would undermine the operations of VERAZ - a credit screening organization.
The *Habeas Data* regulation was later introduced by Law NE 25.326 of October 4, 2000. Such law established the general principles for data protection, the rights of data subjects, regulated issues concerning file users and keepers, data banks and records. The law also has a chapter on controls and sanctions and establishes the personal data protection action.
As the law indicates in article 1, its objective is the “overall protection of the personal data held in files, records, data banks or other technical data processing means, either public or private, intended for reports, to guarantee the right to respect and privacy, as well as access to information in conformity with the provisions of article 43, third paragraph, of the National Constitution.” Its provisions are also applicable to all pertinent data regarding juridical persons.
The law establishes a difference between personal data and sensitive data, stating that the creation of data files is legal provided that the law is observed. Besides, the subject’s consent is required with the exceptions provided by the law. However, the collection and processing of sensitive data is forbidden except if it has been authorized by the law for general interest purposes. The law expressly states that the Catholic Church, other religious associations, political and union organizations may keep files of their members.
The law forbids the international transfer of personal data of any type to countries or international or supranational organizations that do not provide the required levels of protection, with the following exceptions:
- International judicial collaboration;
- exchange of medical data as required by medical treatment or epidemiological research;
- bank or stock exchange transfers regarding such transactions and according to the applicable legislation;
- whenever a transfer has been agreed according to international treaties of which Argentina is party to;
- whenever a transfer is for the purposes of international cooperation between intelligence organizations to combat organized crime, terrorism and drug trafficking.

Among the regulations regarding *habeas data*, the following decrees can also be mentioned: Decree 995/2000, regarding "*Habeas Data*", Publisher in the Official Gazette of 11/2/2000, number 29517; and Decree 1558/2001, on "Personal data protection", published in the Official Gazette of 12/3/2001.

3) PENAL CODE

Articles 153-157 of the Penal Code prohibit the publishing of private communications. In April 1999, a court found that those provisions also applied to electronic mail. Also the Civil Code prohibits "arbitrary interference in another person's life: publishing photos, divulging correspondence, mortifying another's customs or sentiments or disturbing his privacy by whatever means."[52]

b) Brazil

1) BRAZILIAN CONSTITUTION

Brazil does not have a specific law for the purpose of protecting of individuals from the unauthorized collection, use, and disclosure of their personal data held in electronic forms by

II

[51] Law No. 24.745 (23 Dec. 1996).

[52] Art. 1071bis, Cod. Civ.; See: David Banisar and Simon Davies, "*Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*" (1999) 18 (1) *John Marshall Journal of Computer & Information Law* 1, at 15-17.

private organizations.[53] Of relevance, however, is the 1988 Constitution, whose Article 5 guarantees the inviolability of the rights to life, freedom, equality, security, and property, and defines that lawsuits for *habeas data* are free of charge. There are other laws which touch indirectly on the issue of privacy protection in the private sector.

2) Law No. 9507

Law No. 9507, of November 1997, regulates the right of access to information and codifies the procedures of *habeas data.* It considers within the public domain "all registry or databanks containing information which is or could be transmitted to third parties or that is not for the private use of an organ or entity producer or depository of information."

3) Law No. 8078

The focus of Law No. 8078, of September 1990 (*Code of consumer's protection and defence*), is on consumer protection, linked to consumer rights, consumer relations, quality of products and services, and suppliers' responsibilities. In Article 44, the law states that the consumer will have access to personal and consumer related data about his person and respective sources of information. It allows the consumer to review and demand immediate correction of mistaken data.

4) PROPOSED LEGISLATION

In 1996 the Senate of Brazil introduced Bill No. 61 which would have governed the creation and use of personal registers and databanks, whether public or private.[54] The Bill has not become law and was filed on January 1999 with the end of the 1994-1998 Legislature. There is, however, another privacy Bill in the Senate (No. 268 of 1999), already approved by the Senate's Constitution and Justice Committee, that will supersede Law. no. 9507. The new law, if enacted, will govern the structuring and the use of data banks and codify the procedures of *habeas data.* For the purposes of the law, personal data on race, political and religious opinions, beliefs and ideologies, mental and physical health, sexual life, police records, family matters, and profession are considered personal data which can not be released or utilised for any other purpose than that which led to the creation of the databank, except by court order or the person's authorisation. The bill specifies that personal data refers to both physical and juridical persons.

The Privacy Bill mentioned in the preceding paragraph (268 of 1999) is still under consideration in the Senate, and therefore, Law No. 9507 is still in full force and effect with regard to *habeas data*.

c) Canada

While Canada's Constitution, including the Charter of Rights and Freedoms, does not explicitly recognize the right to privacy, the Supreme Court has interpreted Section 8 of the Charter (which deals with search and seizure) to guarantee a right to a reasonable expectation of privacy.[55] Canada has a number of comprehensive laws governing access to and processing of personal data. The Privacy Act[56] as well as the Access to information act[57] apply to federal public sector institutions. In addition, the Personal information and electronic documents act has recently been enacted to regulate data protection in the private sector.

Most provinces have comprehensive laws that cover data processing in the public sector, but Quebec's Act respecting the protection of personal information in the private sector is the only comprehensive law applying to the private sector.

1) PERSONAL INFORMATION AND ELECTRONIC DOCUMENTS ACT

The Personal information and electronic documents act[58] received royal assent on 13 April 2000 and comes into force in Canada on 1 January 2000.[59] The Act's purpose is to establish "rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal

[53] Information on the legislation governing the electronic processing of personal data in Brazil has been provided by Luiz Miguel da Rocha from the Canadian Embassy in Brasília on 27 July 2000.

[54] Privacy Exchange, Legal Library, Proposed/Pending National Legislation, Brazil, "Senate Bill No. 61, 1996": <http://www.privacyexchange.org/>.

[55] *Hunter* v. *Southham* [1984] S.C.R. 159, 160.

[56] Department of Justice, "Consolidated Statutes" <http://canada.justice.gc.ca/FTP/EN/Laws/Title/P/index.html>.

[57] Department of Justice, "Consolidates Statutes", <http://canada.justice.gc.ca/FTP/EN/Laws/Title/A/index.html>.

[58] S.C. 2000, c-5; Canada Gazette, 23(1), <http://canada.gc.ca/gazette/hompar3-2_e.html> [hereinafter PIEDA].

[59] The federal Act provides for several phase-in periods to allow the provinces to adapt to the new legislation. If a province enacts a law that is substantially similar to the federal Act, the organizations or activities covered by the provincial law will be exempted from the federal law.

information and the need to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."[60] While protecting the privacy of personal information, the Act is to support and promote electronic commerce. This new law should help Canada meet the data protection standards established in the European Union Privacy Directive.

The Act will be phased in over a period of three years and will eventually apply to every private organization that collects, uses or discloses personal information in the course of commercial activity, except to activities within provincial jurisdiction where a province has its own law that is substantially similar to the federal Act. To date the province of Quebec is the only jurisdiction in North America which has such a law. The Act does not apply to individuals in respect of personal information collected, used, or disclosed solely for personal or domestic purposes. An exception is also made for organizations collecting, using, or disclosing information whose purpose is journalistic, artistic or literary.[61]

Personal information is defined as "information about an identifiable individual", including race, ethnic origin, colour, age, marital status, religion, education, medical, criminal, employment or financial history, address and telephone number, numerical identifiers such as the Social Insurance Number, fingerprints, blood type, tissue or biological sample, and views or personal opinions.

The Act lists ten principles to govern the collection, use and disclosure of personal information:[62] accountability, identifying the purposes for the collection of personal information, obtaining consent, limiting collection, limiting use, disclosure and retention, ensuring accuracy, providing adequate security, making information management policies readily available, providing individuals with access to information about themselves, and giving individuals a right to challenge an organization's compliance with these principles. These principles are further discussed below.

Accountability

Organizations are responsible for personal information under their control and they must designate individuals to oversee compliance with the Act. Policies and procedures must be implemented, employees trained, and information provided to the public to ensure that personal information is protected. Where information is processed by a third party, an organization is required to use contractual or other means to provide for a comparable level of protection.[63]

Identifying purposes

The purposes for which personal information is processed must be identified and documented, including in cases where previously collected information is used for a new purpose. Preferably, individuals should be informed about the purposes before or at the time of collection but no later than before use of the information.[64]

Consent

Except in limited circumstances, an individual must have knowledge and give his or her consent if personal information is to be collected, used, or disclosed. Consent may be

obtained after collection of the data but no later than before use of the information. To make consent meaningful, the purposes of data processing must be explained to an individual and organizations must make a reasonable effort to ensure that they are understood. The nature and form of consent may vary depending on the sensitivity of the information, the circumstances, and the individual's reasonable expectations. Consent can only be obtained for the processing of data for specified and legitimate purposes. If an organization wishes to use information for a purpose different from that for which it was collected, consent must be obtained again. Individuals are free to withdraw their consent, subject to legal or contractual obligations and reasonable notice.

An organization may collect personal information without the knowledge or consent of an individual only under very limited circumstances. This may be the case as where the collection clearly benefits the individual or where obtaining consent would compromise the

60 PIEDA, Article 3.
61 PIEDA, Article 4.
62 The Act incorporates as Schedule 1 the principles set out in the Canadian Standards Association's *Model Code for the Protection of Personal Information*.
63 PIEDA, Schedule 1, Principle 1.
64 PIEDA, Schedule 1, Principle 2.

information's accuracy. In addition, knowledge and consent are not required for a legal investigation or aid in an emergency that threatens the life, health, or security of an individual, or if disclosure is required by law, for statistical or scholarly purposes or the conservation of records of historical or archival importance.[65]

Limiting collection

The amount and type of information collected must be restricted to what is necessary for identified purposes. All information must be collected by fair and lawful means without misleading or deceiving individuals about the purpose for which information is collected.[66]

Limiting use, disclosure, and retention

Except with the consent of the individual or as required by law, personal information can only be used or disclosed for purposes for which it was collected. Personal information must be retained only as long as necessary to fulfil the identified or required purposes and to allow an individual access to information after a decision has been made. Organizations should develop guidelines and implement procedures for information retention and destruction.[67]

Accuracy

Personal information used by organizations, including information disclosed to third parties, must be as accurate, complete, and up-to-date as necessary for the identified purposes, particularly where this is in the interest of the individual. Limits to the accuracy of the information must be clearly set out. Personal information must not be routinely updated unless required by the purposes for which the information was collected.[68]

Safeguards

Security safeguards must be in place to protect personal information against loss or theft, unauthorized access, disclosure, copying, use or modification. The nature of the safeguards must be appropriate to the sensitivity, amount, distribution, format, and storage of the information. The methods of protection should include physical measures such as locked filing cabinets, organizational measures such as security clearances, or technological measures such as computer passwords. Employees must be aware of the need to protect the confidentiality of personal information, and care must be taken in the disposing of data to prevent unauthorized access.[69]

Openness

Information about an organization's policies and practices related to the management of personal information must be provided to the public. Such information must include the name, title and address of the person in charge of compliance with the Act and to whom complaints can be brought; a description of the nature of personal information held by the organization; the means of gaining access to that information; and what information is provided to related organizations such as subsidiaries. This information must be both easy to obtain and understand.[70]

Individual access

Individuals have a right to access their personal information, challenge its accuracy

and completeness and have it corrected. Access must be granted unless it would compromise personal data of other individuals, be extremely costly, or is prohibited for legal, security, commercial proprietary reasons, or because of solicitor-client privilege. Organizations must inform an individual about what personal information they possess, how it is used, and to which third parties it has been disclosed. Access to information requests must be answered within a reasonable time period, which would normally be 30 days. If a request for access to information is refused, the individual must be informed in writing about the reasons and any other recourse available under the Act.[71]

II

[65] PIEDA, Article 7; Schedule 1, Principle 3.
[66] PIEDA, Schedule 1, Principle 4.
[67] PIEDA, Schedule 1, Principle 5.
[68] PIEDA, Schedule 1, Principle 6.
[69] PIEDA, Schedule 1, Principle 7.
[70] PIEDA, Schedule 1, Principle 8.
[71] PIEDA, Articles 8-9; Schedule 1, Principle 9.

Challenging compliance

Individuals have a right to bring a complaint about an organization's lack of compliance with the Act to the designated official.[72] If an individual cannot settle a dispute with the designated official, he or she can complain to the federal Privacy Commissioner who performs the functions of an ombudsman. The Privacy Commissioner receives complaints concerning contraventions of the Act, conducts investigations, and attempts to resolve complaints through persuasion, mediation and conciliation. He or she has powers to seek and examine relevant information when conducting an investigation and may enter the premises occupied by an organization, examine relevant records, and interview individuals. After an investigation, the Privacy Commissioner may write a report with appropriate findings and recommendations. Persons who hinder the Commissioner's investigation, destroy documents, or move against whistle blowers are guilty of an offence and may be fined up to $100,000. The Privacy Commissioner can also audit the information management practices of an organization and make the results public. The Commissioner's tasks include public education programs and research.[73]

The Commissioner has no power to compel an organization to act on the findings or recommendations of a report. If a matter remains unresolved, an individual may, however, bring a complaint to the Federal Court of Canada within 45 days of receiving a report from the Commissioner. The Commissioner may appear on behalf of a complainant or as a party to the hearing. The Court may prescribe corrective measures to the organization involved and award damages to the complainant if appropriate.[74]

2) OTHER FEDERAL LEGISLATION

Other legislation by the Canadian Government which provides for privacy protection includes the Criminal Code which prohibits the unlawful interception of private communications.[75] In addition, there are sectoral laws like the Bank Act[76], the Insurance Companies Act[77], and the Trust and Loan Companies Act[78], among others, which provide for the protection of privacy.[79]

3) QUEBEC: ACT RESPECTING THE PROTECTION OF PERSONAL INFORMATION IN THE PRIVATE SECTOR

With the enactment of the Act respecting the protection of personal information in the private sector in 1993, the Province of Quebec became the first jurisdiction in North America to provide for comprehensive legislation governing the protection of personal information in the private sector. The Act regulates the collection, use, and dissemination of personal information and grants individuals the right to have access to their personal data and to have them corrected if applicable. Complaints can be brought to the Commission d'accès à l'information.

c) Chile

1) CHILEAN CONSTITUTION AND OTHER LAWS

Privacy and secrecy of communications are protected under Article 19 of Chile's Constitution of 1980. Law No. 19, 423 prohibits undisclosed taping, telephone intercepts, and other surreptitious means. Information obtained in such a way can only be disclosed by judicial order.[80]

2) ACT ON THE PROTECTION OF PERSONAL DATA

The *Act on the protection of personal data*[81] of August 1999 is the first comprehensive personal data protection law applying to the public and the private sector in Latin America. The Act regulates electronic as well as manual processing of personal data. The following principles are ensured by the Act:

II

[72] Schedule 1, Principle 10.
[73] PIEDA, Articles 11-13. The web site of Canada's Privacy Commissioner can be found at: <http://www.privcom.gc.ca>.
[74] PIEDA, Articles 14-17.
[75] Criminal Code, c-46, " 184, 193.
[76] R.S.C. ch. B-101, " 242, 244, 459.
[77] R.S.C. ch I-11.8, " 489, 607.
[78] R.S.C. ch T-19.8, " 444.
[79] See David Banisar and Simon Davies. *Op.cit.*, p.26-30.
[80] See . David Banisar and Simon Davies. *Op.cit;,* p. 30-31.
[81] Online: Privacy Exchange, National Omnibus Laws: <http://www.privacyexchange.org/>.

63

Fair Information practices

Data processing can only occur in accordance with internationally recognized fair information practices.

Consent

The processing of personal data requires express written consent from the data subject, unless authorized otherwise by law. Consent can be revoked (but not retroactively) in writing. There is no requirement to obtain consent if data are publicly available; used only for internal purposes; shared with associates or affiliates; or used for statistical or rating purposes.

Personal data can only be used for the purpose(s) for which they were collected. Individuals may object to the use of personal data for advertising or market research.

Sensitive data

Sensitive data, including those revealing formation about, race, ethnic origin, political opinion, philosophical or religious belief, physical or mental health, sexual life, and personal habits, may only be processed if authorized by law, express consent is given by the individual or if processing is required to determine a person's medical treatment and health benefits. Personal medical information may only be disclosed with the patient's express, written consent.

Accuracy and security

Data processors must ensure that data are accurate, complete, up-to-date, and secure.

Access and transparency

Individuals must be informed about who collects personal information, what information is collected for what purpose, and which third parties are to receive the information. Every six months, they are also entitled to a free copy of the information held by an organization. Individuals may not only request the correction of personal data but also its blocking or deletion if the data 1) have been voluntarily supplied; 2) are outdated or obsolete; 3) are being used for commercial purposes.

Enforcement

While there is no provision for an independent data protection authority, complaints can be made to the courts.

Chile has not enacted any other legislation after doctor Fried's report. Also, other decrees declaring certain municipal acts and documents as secret due to private interests that they may involve have been enacted. For example, this should be the case of Decree 7779/2000, Test to the Regulation of Personal Data Banks held by Public Organizations.

e) Mexico

1) MEXICAN CONSTITUTION

While the Mexican Constitution does not have specific provisions relating to the disclosure of electronic data, it does have general articles which refer to the right to information and to the freedom of the press.[82] Article 6 states that the right to information will be guaranteed by the State. Article 7 limits freedom of the press with respect to privacy, morality, and the public peace.

Article 16 of the Mexican Constitution states:

No one shall be molested in his person, family, domicile, papers or possession except by virtue of a written order of the competent authority stating

the legal grounds and justification for the action taken.
.....
Administrative officials may enter private homes for the sole purpose of ascertaining whether the sanitary and police regulations have been complied with, and may demand to be shown the books and documents required to prove compliance with fiscal rulings, in which latter cases they must abide by the
II
[82] Information on the state of Mexican law was provided by Heather Jeffrey and Gilian Moran from the Canadian Embassy in Mexico on 24 July 2000.

provisions of the respective laws and be subject to the formalities prescribed for cases of search.
2) LEGISLATION
The Federal Law on Transparency of and Access to Public Information published on June 11, 2002, contains a chapter intended for the protection of personal data. It provides for the access to and possibility of correcting personal data. The provisions of the Constitution are complementary as well as some sectoral laws, including the Federal Copyright Law.
Article 109 of the Federal copyright law (Ley federal del derecho de autor) makes it illegal to sell or offer personal information contained in an electronic database without permission of the individual. The text of Article 109 is as follows:
The access to private information on persons contained in databases to which the preceding Article refers as well as the publication, reproduction, release, public communication and transmission of said information, shall call for the prior authorization of the persons involved.
Any investigations carried out by the authorities entrusted with procuring and imparting justice, in accordance with the respective legislation, as well as the access to public archives by persons authorized by law, shall be exempt from the foregoing, provided that the consultation is made pursuant to the respective procedures.
f) Peru
1) POLITICAL CONSTITUTION OF PERU
The Peruvian Constitution of 1993 establishes in article 2, paragraph 5, the right of "any public entity to request without any explanation and to receive the information it may require, within the legal term, at the cost that such request may imply. Exceptions to this provision are the information affecting personal privacy and those expressly excluded by the law or for national security reasons. Bank secrecy and fiscal reserve may be disclosed at the request of a judge, the Attorney General or an investigative commission of the Congress based on the law and provided that it is relating to the investigation". The following paragraph of the same article also establishes that "information services, computerized or not, public or private, shall not provide information affecting personal and family privacy".
In turn, article 200 of the same constitutional law establishes *habeas data* as a constitutional guarantee, prescribing that it "proceeds against the act or omission, by any authority, officer or person, that violates or threats the rights to which Article 2, paragraphs 5) and 6) of the Constitution refer". *(Paragraph reformed by Law Nº 26.470 of June 12, 1995.)*
2) LEGISLATION
The Constitutional Procedural Code (Law No. 28237) regulates the proceedings for *habeas data* action since 2004. Article 60 of the Code establishes the right to resort to such process to have access to information held by any public entity as well as to know, update, include and suppress or rectify personal information or data stored in files, data banks or records of public entities or private institutions. It also contemplates the possibility of suppressing or preventing the disclosure of sensitive or private data which may affect the constitutional rights of an individual.
We must also mention Law 27489 of June 2001 that regulates information disclosure by private risk rating companies (regarding creditworthiness, indebtedness and payment records) and the protection of the information subject as well as the enactment of a law in April 2005 that regulates the use of unsolicited commercial electronic mail (spam).
3) PENAL CODE
Under Article 154 of the Penal Code of Peru "a person who violates personal or family

privacy, whether by watching, listening or recording an act, a word, a piece of writing or an image using technical instruments or processes and other means, shall be punished with imprisonment for not more than two years. Article 151 of the Penal Code provides that "a person who unlawfully opens a letter, document, telegram, radio telegram, telephone message or other document of a similar nature that is not addressed to him, or unlawfully takes possession of any such document even if it is open, shall be liable to imprisonment of not more than 2 years and to 60 to 90 days' fine.

65

g) United States

The right to privacy is not explicitly protected in the US Constitution. The Supreme Court held that a limited constitutional right to privacy arises out of the Bill of Rights in relation to government surveillance. The right to privacy in the private sector is only guaranteed where there is legislation. There is no privacy oversight authority in the United States. The Office of Management and Budget plays a policy role in the federal public sector and the Federal Trade Commission oversees consumer credit information and fair trading practices.[83] The United States does not have a comprehensive law controlling access to and the protection of information and personal data held by private organizations.[84] Instead the United States has legislated on a sectoral basis and relies heavily on self-regulation of the private sector. Legislation regulating privacy protection in the private sector includes, among others, the following acts:

1) Cable communications policy act

The Cable communications policy act[85] (1984) regulates the use of cable television subscriber records. Consumers must be informed about the nature of the information collected and its use. Identifiable information such as viewer choices may not be disclosed without written consent. Information must be accurate and procedures for corrections must be in place. Consumers must be informed at least once a year about the "nature, frequency, and purpose" of information stored and disclosed. Actual and punitive damages may be obtained through court action.

2) Children's online privacy protection act

The Children's online privacy protection act (1998)[86] applies to information concerning children collected on-line. The Act requires that parents must consent before data on children under the age of 13 can be collected or disclosed.[87] Parents must also be given access to data collected and can prevent the further use of the information. Operators of commercial websites must inform parents about their information practices and must maintain confidentiality, security and integrity of the information.

3) Electronic communications privacy act

The use of electronic communications, including voice, video, and data communications, is regulated by the Electronic communications privacy act[88] (1986). The Act prohibits the unauthorized interception, acquisition, or disclosure of electronic communications, including those stored on a computer, unless the communication is readily accessible to the general public. It applies to the public as well as the private sector. Yet, the Act allows for several exceptions. Computer system operators for example may access stored data and divulge information accidentally obtained to government authorities. Since a system can be configured to store all messages that pass through it, the system operator may have access to all messages that pass through. Violations of private communications carry with them potential criminal and civil damages.[89]

4) Fair credit reporting act

Under the Fair credit reporting act[90] of 1970, the collection and use of information of credit reporting agencies is regulated. The Act applies to the activities of those who supply the information to credit agencies, to the credit agencies themselves, and users of credit information. Credit agencies must ensure that their information is accurate and provide for correction procedures. Their records must be available to consumers. Information can only be released to authorized customers who must notify the consumer if adverse action is taken based on a credit report. Users must also inform the consumer about the source of the credit information. If information is incomplete or inaccurate, the consumer can request that the matter be investigated free of charge by the credit agency. The Act is administered by

II

[83] See David Banisar and Simon Davies. *Op.cit.* p.108-111.

[84] The federal government's handling of personal data is regulated by the *Privacy Act* (1974), 5 U.S.C. ' 552a (1994).

[85] 47 U.S.C. ' 551.
[86] Online: United States, Federal Trade Commission: “Legal Framework, Statutes Enforced or Administered by the Commission, Statutes Relating to Consumer Protection Mission” <http://www.ftc.gov/ogc/stat3.htm>.
[87] Information for the protection of children using the internet and filtering programs are available at a web site called "getNetWise": <http://www.getnetwise.org/>.
[88] 18 U.S.C. ' 2510-2520, 2701-2709 (1997).
[89] See: Domingo R. Tan, “Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union” (1999) 21(4) Loyola of Los Angeles International and Comparative Law Journal, 661.
[90] 15 U.S.C. ' 1681-1681(u); Federal Trade Commission: <http://www.ftc.gov/os/statutes/fcra.htm>.

the Federal Trade Commission which has procedural, investigative and limited enforcement powers. Aggrieved persons can also bring cases to court and sue for actual and punitive damages.

5) Right to financial privacy act

The Right to financial privacy act[91] regulates the transfer of financial records. Generally banks are prohibited from disclosing clients’ financial records without a court order. Individuals are generally given the opportunity to challenge access of federal investigators to financial records. Relief for actual and punitive damages may be sought in the courts.

6) Video privacy protection act

Video rental or sales information is protected under the Video privacy protection act[92]. The Act prohibits the release of consumers’ names, addresses, and titles of videos rented or bought. Customers must be given an opportunity to opt out of marketing schemes. Aggrieved parties can sue in the courts.

While the US Government has regulated data protection in parts of the private sector, major legislative gaps continue to exist, for example, with respect to medical records, bank records and the internet. Some privacy protection is available through state legislation and through the courts, the tort of privacy was first adopted in 1905 and is now available in almost all states as a civil right of action.[93] The general approach, however, remains that the private sector should regulate itself through codes of conduct and market forces. There are a number of industry-based organizations which have developed codes of conduct. These include, among others, the “Information Technology Industry Council”, the “Interactive Services Association”, the “Online Privacy Alliance” and the “American Electronics Association”.[94]

h) Uruguay

1) CONSTITUTIONAL REGULATIONS

Article 28 of the Constitution of Uruguay establishes the following: “Personal documents and personal correspondence by letter, telegraph or of any other kind are uninfringeable and shall never be searched, inspected or intercepted in any way except according to the laws intended for the general interest”. This article should be jointly interpreted with arts. 7, 72 and 332.

2) LAWS AND OTHER REGULATORY INSTRUMENTS

The protection of personal data was specifically regulated by Law NE 17.838. Such law established the principle of the need to obtain the express and informed consent of the data subject to collect data which are not of commercial nature, excepting from this requirement certain data of this nature (article 4) defined as “lists containing data limited to full names, personal identity documents or taxpayer’s identification record, nationality, marital status, name of spouse, type of marriage, date of birth, address and telephone number, occupation, profession and legal residence”.

The law expressly establishes that the following data, among others, are not of commercial nature:

- personal data originated from the exercise of the freedom to issue an opinion, to inform,
- those relating to surveys, market studies, or similar,
- sensitive data relating to personal privacy regarding the racial and ethnic origin of a person as well as his/her political preferences, religious or philosophical or moral beliefs, union affiliation or information regarding his/her physical health or sexuality and any other area reserved to individual liberty.

[91] 12 U.S.C. sec. 3401 et seq.
[92] 18 U.S.C. ' 2710. This Act was passed in response to media reports about video rental records of Judge Robert Bork’s family

during Supreme Court nomination hearings.
[93] See David Banisar and Simon Davies. *Op.cit*. p 108-111.
[94] For data protection laws in the United States, see also: Organization for Economic Cooperation and Development; Directorate for Science, Technology, and Industry; Committee for Information, Computer and Communications Policy; Working Party on Information Security and Privacy; Inventory of Instruments and Mechanisms Contributing to the Implementation and Enforcement of the OECD Privacy Guidelines on Global Networks,@ DSTI/ICCP/REG (98)12/FINAL, (19 May 1999) at 47-50.

The general principle applicable to these data is that the express and prior conformity of the data subject is required and is limited to the purpose and scope of the register in question.
The Law also establishes a *habeas data* mechanism and a controlling body for the case of violations of the rules of protection applicable to both types of data. It establishes that everyone will have the right to file an effective action to know his/her personal data and their purpose and use, being held in public or private records or data banks and in case of error, falseness or discrimination, to demand rectification, suppression or whatever may apply.
All personal data subjects with previous due identification with personal identification document will be entitled to obtain all personal information held in public of private databases. This right of access will be exercised free of charge and at intervals of not less than six months, unless a new legitimate interest has arisen according to the legal regulations. Likewise, in case it applies due to error in the information or false information, such individual will be entitled to request the rectification, updating and elimination of his/her personal data. In case the person in charge of the database fails to comply with the obligation to rectify within the term established by the law, the interested party is entitled to bring a *habeas data* action.
On its part, art. 694 of law 16736 established the right of access to the various data banks.
There are other sectoral provisions among which are the bank secrecy regulations (decree law 15322), secrecy in Disciplinary Proceedings, Registry of Summary Proceedings, competence of the Civil Service Office of the Presidency of the Republic, arts. 17, 40 and 42 of Decree 258/92, Decree 396/03 regarding Medical Records and laws 14005 and 17668, regulating cloning and organ transplants, establishment of data banks and the necessary secrecy to protect donor's rights. Also, Law 16616 regulates the national statistical system by expressly establishing some principles to be kept in mind to safeguard the principles of information privacy and self-determination.
Likewise, there are regulatory rules that establish the free flow of information (art. 14 of Decree 500/91), electronic dossiers for Central Ministration officials (Executive Branch), Decree 385/99, and storage methods of electronic documents, Decree 83/001.
Finally, Supreme Court of Justice meeting 7564 of February 2006 regulates the protection of personal data held in the databases of such entity.
3) PENAL CODE
From the penal viewpoint, the Penal Code establishes the violation of written correspondence and telegraphic communication and the possession of secret documents by fraudulent means (arts. 296, 297 and 300).
i) Colombia
Article 15 of the Constitution of Colombia establishes the following: "Every individual has the right to personal and family privacy and to a good name and the State must respect such right and ensure that others respect it. Likewise, they have the right to know, update and rectify all information collected from them in databanks and files of public and private entities.
Data collection, processing and flow, liberty and other guarantees established in the Constitution will be observed.
Correspondence as well as other types of private communication is inviolable. It can only be intercepted or searched by way of court order in the cases and instances that they law may provide. (…)
For judicial or tax purposes and for the purposes of inspection, surveillance and intervention by the State, the presentation of accounting records and other private documents may be required according to the law".
Notwithstanding the constitutional provision, Colombia does not have a legal entity engaged in the comprehensive regulation of matters relating to the protection of data,

although there are some sectoral provisions scattered in several legal entities such as the protection of data relating to medical conditions and inviolability of correspondence. In the past, several bills were submitted but were not approved. For the present term of office, there are plans to discuss in the Colombian Congress the bill “Statutory law in the matter of *habeas data*”, to establish regulations for article 15 of the Constitution.
68
Besides, the Colombian Constitutional Tribunal has played an active role since it has pronounced more than one hundred relevant sentences guaranteeing compliance with habeas data and the protection of personal data, stating some relevant juridical principles. The Penal Code also provides for the establishment of conducts such as the illicit violation of communications and the supply, sale or purchase of instruments intended for the interception of private communications.

j) Paraguay

1) CONSTITUTION OF 1992

Article 135 of the Constitution of Paraguay specifically contemplates the figure of *habeas data* in the following terms: “Every individual is entitled to access to personal information or data or regarding his/her assets held in official or private records as well as to be aware of their use and purpose. Every individual will be entitled to request to the competent magistrate, the update, rectification or destruction of such data if they contain errors or illegitimately affect the rights of the individual”.

2) LEGISLATION

Paraguay has a law that regulates information of private nature, Law No. 1682/01, as modified by Law 1969/02. The object of this legislation is to “regulate the collection, storage, distribution, publication, modification, destruction, duration, and in general, the processing of personal data held in files, registries, data banks or any other technical means for the processing of public or private data intended for the supply of reports, in order to guarantee the full exercise of the data subject’s rights”. The laws in question also establish the right of every individual to access the data held in public registries.

The legislation in question also establishes the conditions under which data relative to physical or juridical persons regarding the status of their assets, economic solvency or fulfillment of their commercial and financial obligations may be published or disseminated. The laws specifically provide for three assumptions:

- with previous authorization in writing by the affected party regarding debts that are not part of a judicial claim;
- the dissemination obeys to compliance with specific legal provisions;
- the information in question is held by public sources of information.

The law also provides for the obligation to update personal data held in the registries of individuals or entities that process information, and establishes the corresponding sanctions which basically consist in fines.

3) PENAL CODE

Chapter VII of Title I of Book 2 of the Penal Code of Paraguay contains a series of provisions relevant to data protection such as those establishing the violation of personal privacy, violation of the right to communication and self-image, violation of communication secrecy or disclosure of secrets of private nature.

k) Ecuador

1) CONSTITUTION

Article 94 of the Constitution of Ecuador provides for the following: “Every individual will have the right to access documents, data banks and reports relating to his/her own personal data or assets held in public or private entities, as well as to be aware of their use and purpose. Every individual will be entitled to request to the respective officer, the update, rectification or destruction of such data if they contain errors or illegitimately affect his/her rights. If the lack of attention to this matter causes any damage, the affected party is entitled to compensation. The law will establish a special procedure to have access to personal data held in files relating to national defense”.

Article 276 of the same Constitution establishes that the Constitutional Tribunal will have jurisdiction in hearings regarding “resolutions denying …. *habeas data*…”.

2) LEGISLATION

The Constitutional Control Law of 1997 regulates some of the procedural aspects of the institute, particularly in Title II, Chapter II. Article 35 provides for *habeas data* as a resort

to:
69
- obtain from the data subject complete, clear and truthful information;
- make that whoever holds the information will rectify, eliminate and will not disclose it to third parties;
- obtain certifications or verifications stating that whoever holds the information has rectified, eliminated or has not disclosed it.

Article 9 of the Electronic Commerce Law provides protection for the collection, transfer, use and transmission of personal data obtained by any means and specifically through data bases. The violation of these provisions is sanctioned as a crime.

l) Costa Rica

1) CONSTITUTION

The Constitution of Costa Rica does not provide any specific rule relating to the protection of personal data or information self-determination as a specific juridical asset subject to protection. Article 24 establishes, however, the right to privacy, extending the protection to private communications and documents

2) LEGISLATION

There is no legal regulation of general and comprehensive nature regarding this matter, although some bills have been introduced with the purpose of regulating it, for example, with the intention to introduce an additional chapter regarding *habeas data* to the Constitutional Jurisdiction Law. The Supreme Court has also drafted a bill on the matter. The protection of data is currently addressed through the general appeal system.

m) Guatemala

Articles 30 and 31 of the Constitution of Guatemala regulate the matter relating to making public the access to administrative acts and files and records, however, only files and records of governmental nature are mentioned. Several bills have been introduced throughout the years regarding *habeas data* and the protection of personal data as part of the matter regarding access to information, however, no law has been enacted so far.

n) Panama

The Constitution of Panama does not provide a specific rule addressing *habeas data*.

Law 6 of January 22, 2002, regulates *habeas data* along with public administration transparency, even though the former only applies to public and private entities that by virtue of a concession provide public services. The law establishes the right of the affected parties to the correction of elimination of incorrect or outdated information. The Law of May 25, 2002, also regulates the information service on matters relating to credit solvency and includes some provisions for the regulation of the activity of entities engaged in the collection of data relating to personal economic solvency or credit history.

o) Venezuela

1) CONSTITUTION OF VENEZUELA

Article 28 of the Constitution of 1999 expressly refers to the protection of personal data: “Every individual has the right to access documents and data relating to his/her own personal data or assets held in public or private entities, with the exceptions provided for by the law and to be aware of their use and purpose, and request to the court having jurisdiction the update, rectification or destruction thereof if they contain errors or illegitimately affect the individual rights of the individual. Likewise, an individual will also have access to documents of any nature containing information of interest to communities or groups of persons, with the exception of the secrecy of the information sources for the press and other professions that the law may specify”.

Article 60 also establishes the protection of the honor, private life, self-image, confidentiality and reputation, providing that the law will limit the use of information to the effect of guaranteeing personal and family honor and privacy to all citizens.

Finally, article 281, paragraph 3, attributes to the people’s ombudsman the faculty to file for *habeas data* action.

2) Legislation

Chapter 3 of the Special Law against Computer Crimes establishes provisions relating to personal and communications privacy, establishing the conduct in violation of these juridical assts as a crime.

70

II. REGULATION OF TRANSBORDER DATA FLOWS

1. Background

As it is the case with many other international transactions, the flow of personal data across borders by electronic means, particularly the internet, raises numerous jurisdictional questions. The identification, assignment and enforcement of jurisdiction may pose considerable difficulties. The following example may be illustrative of the problem: personal financial information about an individual of Country A is collected by a credit bureau. The information is stored on a computer in Country B and also at the bureau's headquarters in Country C. The individual has reason to believe that some of the information may not be correct and wants to access it. The laws of Country A provide a right of access to such information if it is held in Country A. In this case, however, the information is not held in Country A. Country B has a similar law but it applies only to the public sector and thereby excludes recourse against a private credit bureau. Also Country C has data protection laws, but they apply only to its own citizens. Recourse is not possible because the individual is not a citizen of Country C. Thus, even though the three countries have data protection laws, a lack of jurisdiction prevents recourse for the individual concerned.[95]

Establishing a jurisdictional rule to cover Internet sites is rather difficult without creating conflict, given that so many individuals belonging to many distinct communities use the Internet. Additional problems are posed by technology, for example when trying to determine who should regulate a particular internet server. One approach could be to allocate jurisdiction according to the country of the domain name registration. Yet, websites could be registered under several domaines such as the ".com" domain as well as the ".uk" domain. Jurisdiction on the basis of the IP number is also difficult because two different websites could use the same IP-number. Even the establishment of jurisdiction based on the physical location of the server is problematic. Such a policy could encourage the placement of servers in locations where laws are favourable to the owner, a "cyberhaven". In any event, any assertion of jurisdiction based on the current technological configuration of the internet will likely be doomed as technology evolves further.[96]

The globalization of data processing renders privacy protection increasingly difficult without the application of extra-territorial jurisdiction. Under traditional international law, however, most States oppose extraterritorial measures that contradict or undermine the laws or clearly enunciated policies of another State exercising concurrent territorial jurisdiction over the same conduct.[97] There may be a need to devise new ways of dealing with the issue of state jurisdiction to deal with the challenges posed by the Internet and other global networks. Some attempts to address transborder data flows, including jurisdictional aspects, have been made at the international as well as domestic level.

2. International instruments

The issues of jurisdiction, transborder data flows and international cooperation have been addressed in a limited and general way by the OECD Guidelines, the Council of Europe Convention, and the UN Guidelines. A more detailed approach to the transboundary flow of data was adopted in the EU Directive.

a) OECD Guidelines

The OECD Guidelines provide some basic principles for dealing with the flow of personal data across borders and legitimate restrictions for the purpose of privacy protection. The Guidelines recommend a country should take all reasonable steps to ensure that transborder flows of personal data are "uninterrupted and secure". A country "should refrain from restricting transborder flows of personal data" unless the re-export of data would circumvent its domestic privacy legislation or the other country provides "no equivalent protection." The OECD Guidelines reinforce that "countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which

[95] "Conflicting Assertions of National Jurisdiction over Information Matters." Noes for a Speech by J.T. Fried before the Media and Communications Law Section of the Canadian Bar Association, Ottawa, 11 October 1984.

[96] For a discussion of jurisdiction over the internet in the context of European conventions see: Agne Lindberg, Delphi Lawyers, "Jurisdiction on the Internet: European Conventions," 7 January 1998, at the web site Privacy Exchange, Conference Presentations and Papers, <http://www.privacyexchange.org/>.

[97] For a discussion of the principles of jurisdiction see: Pierre Trudel, "Jurisdiction over the Internet: A Canadian Perspective" (1998) 32(4) International Lawyer 1027 at 1029-1047.

would create obstacles to transborder flows of personal data that would exceed requirements for such protection."[98]

The OECD Guidelines encourage international cooperation by ensuring "that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries." Members are called upon to exchange information related to the Guidelines and to facilitate "mutual assistance in the procedural and investigative matters involved." Finally, countries should develop "principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data."[99]

b) Council of Europe Convention

The Council of Europe Convention states that A[a] Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorization transborder flows of personal data going to the territory of another Party. Yet, a Party to the Convention may block the transborder flow of data "insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection." Similarly, a Party may prohibit the cross-border transfer of personal data where "the transfer is made from its territory to the territory of a noncontracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation ..."[100] In short, data transfers can be blocked to countries which do not provide an equivalent standard of protection.

In order to facilitate the transborder flow of data, the Convention requires each Party to designate a national data protection authority which provides information on its laws and administrative procedures in the field of data protection to other Parties.[101] In addition, each Party is required to assist persons resident abroad to exercise their rights.[102] The Convention establishes a Consultative Committee which represents member States and makes proposals as to the application and improvement of the Convention.[103]

The Draft Protocol produced by the Consultative Committee requires the supervisory authorities established under the Protocol to cooperate with one another in the performance of their duties, particularly through the exchange of information.[104]

The Protocol also addresses the issue of transborder data flows to a recipient which is not subject to the jurisdiction of a Party to the Convention. It states that such transfers of personal data are permitted "only if that State or organization ensures an adequate level of protection for the intended data transfer."[105] Exceptions to this rule are only allowed:

a) if domestic law provides for it because of specific interests of the data subject, or legitimate prevailing interests, especially important public interests, or

b) if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law.[106]

The provisions of the Draft Protocol with respect to the transfer of personal data to third countries are similar to those of the EU Directive.

c) United Nations Guidelines

The UN Guidelines address the issue of transborder data flows in Article 9 which states:

When the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned. If there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands.

II

[98] OECD Guidelines, Part Three.
[99] OECD Guidelines, Part Five.
[100] Council of Europe Convention, Article 12.
[101] Council of Europe Convention, Article 13.
[102] Council of Europe Convention, Article 14.
[103] Council of Europe Convention, Articles 18-20.
[104] Draft Protocol, Article 1.
[105] Draft Protocol, Article 2.
[106] Draft Protocol, Article 2.

As in the OECD Guidelines, limitations on the crossborder flow of data are only permitted if the required standards of privacy protection are not met. Measures must be proportionate to the need of protection required.

d) European Union Privacy Directive

One of the major objectives of the EU Directive was to address the transborder flow of personal data and to create a common European market. Article 1(2) of the EU Directive requires that countries of the European Union "shall neither restrict nor prohibit the free flow of data between Member States." Given that all EU States are required to provide a roughly equivalent level of protection for personal data as a result of the EU Directive, limitations on the free movement of data merely for reasons of privacy protection are not permitted within the Union.

Chapter IV of the EU Directive deals with the Transfer of personal data to third countries. EU countries must block the transfer of personal information to non-member States that do not offer an "adequate" level of protection. Article 25 of the EU Directive states:

1. The member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

Decisions about the adequacy of a third country's data protection regime under the EU Directive are first made at the level of national authorities. The EU member States and the European Commission are required to share information with each other about cases where a third country does not properly protect personal data.[107] If the Commission finds that a third country does not offer an adequate level of protection, EU member States are required to prevent the transfer of personal data.[108]

Article 26 of the EU Directive provides the following exceptions to the rule that personal data cannot be transferred to countries providing an adequate level of protection:

a) the data subject has given his consent unambiguously to the proposed transfer; or

b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

e) the transfer is necessary in order to protect the vital interests of the data subject; or

f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

The transfer of personal data to a third country that does not provide adequate privacy protection is also permissible "where the controller adduces adequate safeguards with

[107] EU Directive, Article 25(3).
[108] EU Directive, Article 25(4).

respect to the protection of the privacy", for example through "appropriate contractual clauses".[109]

Where a third country does not provide adequate privacy protection, the Commission may enter into negotiations "with a view to remedying the situation".[110] Given the importance

of the EU in the global exchange of data, the EU Directive has potentially significant consequences outside the Union. Where third countries do not provide sufficient legislation to protect personal data in the private sector, public authorities or even individual businesses may be forced to undertake negotiations with the Commission with a view to demonstrating their compliance with the EU rules.

The EU Directive encourages cross-border cooperation within the European Union by stipulating that a national "authority may be requested to exercise its powers by an authority of another Member State" and that "supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information."[111]

3. National legislation

Most States do not have specific legislation dealing with the transborder flow of personal data. However, the data protection laws of some countries require that the release of personal data to foreign States can take place only if certain conditions are met. Usually the foreign State or the recipient organization must guarantee a minimum level of privacy protection. Some laws also make provisions for cooperation with other data protection or law enforcement authorities.

A) ARGENTINA

Argentina has no specific laws governing the flow of data in electronic form across international borders.[112] However, the proposed *habeas data* bill No. 606 of 1998 approved by the Argentine Senate forbids the transfer of personal data of any kind to other countries or to international or supra-national bodies which do not provide adequate levels of protection. Exceptions to this are exchange of data with purposes of international judicial cooperation, medical data if the treatment of a patient requires it or in the course of epidemiological research, bank or stocks transfers, when the transfer is done according to international treaties to which Argentina is a signatory, or when it is part of international cooperation among intelligence agencies with the purpose of fighting organized crime, terrorism and drug trafficking. It is not clear how this will be applied to the internal operations of transnational corporations, or to the operations of business level transactions.

B) CANADA

Canada's Privacy Act, which applies to the public sector, provides (in Article 8) for the transboundary disclosure of personal information:

f) under an agreement or arrangement between the Government of Canada or an institution thereof and the government of a province, the government of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, for the purpose of administering or enforcing any law or carrying out a lawful investigation;

Unlike *the Privacy Act, the Personal information and electronic documents act does not address the issue of transborder flow of information or cooperation in specific terms, but organizations in Canada will still be held responsible for the proper protection of personal data even when data are transmitted across borders (accountability principle).*[113] *Quebec's Act respecting the protection of personal information in the private sector provides in Section 17 that when communicating data outside Quebec, an enterprise must* take reasonable steps to ensure that the data will be used only for specified purposes and that the data subject is given an opportunity to object to use of the data for solicitation.

II

[109] EU Directive, Article 26.
[110] EU Directive, Article 25(5).
[111] EU Directive, Article 28.
[112] Information on the legislation governing the electronic processing of personal data in Argentina has been provided by Hartmuth Kroll from the Canadian Embassy in Buenos Aires on 26 July 2000.
[113] Discussion with Ken Huband, Privacy Policy, Industry Canada on 1 August 2000.

III. APPROACHES TO DATA PROTECTION

1. Common data protection standards

One approach states have taken at the international level is to agree on a minimum level of convergence of national data protection regimes. The European Union has taken the most forceful approach by requiring its member States to harmonize their data protection legislation. While national laws need not be identical under the EU Directive, reasonably

high-level standards must be met by all countries in order to create a common European market for the flow of data. In addition, a supranational organization, the European Commission, continues to play an important coordinating role and ensures that the Union's standards are not undermined by data transfers to third countries which do not meet the required standards. While presenting a significant challenge, this kind of harmonization of laws could be extended beyond the European Union through bilateral treaties or multilateral conventions.[114]

Indeed, all the international instruments discussed above have attempted to encourage the enactment of laws that provide a consistent and comparable level of privacy protection in the area of personal data processing. While the OECD Guidelines and the UN Guidelines represent non-binding recommendations on which to build data protection regimes, the Council of Europe Convention and particularly the EU Directive are legally binding instruments requiring states to pass laws establishing certain minimum standards in privacy protection. As a result of the Council of Europe Convention and the EU Privacy Directive, most European States introduced privacy protection regimes.[115]

The hope is that by agreeing on a minimum level of common data protection principles, states are no longer required to impose restrictions on transborder data flows. The international instruments discussed above allow for limitations to the free flow of data only in certain exceptional cases. The OECD Guidelines refer to countries that do not "substantially observe" the OECD Guidelines or fail to provide "equivalent protection"; the UN Guidelines make reference to a lack of "comparable safeguards"; the Council of Europe Convention requires the absence of "equivalent protection"; and the EU Directive provides for restrictions on data flows outside the Union where third countries do not offer an "adequate level of protection".

Where the required level of protection is not met, certain limited measures of control can be applied. The OECD Guidelines discourage measures which "in the name of the protection of privacy and individual liberties which would exceed requirements for such protection." The UN Guidelines recommend that restrictions be imposed "only in so far as the protection of privacy demands". The European Council Convention and the EU Directive clearly provide for a blocking of the movement of personal data to countries where sufficient protection is not assured.

The EU Directive imposes the strongest limitations on the transborder flow of data. Article 25 of the EU Directive obliges, rather than permits, EU member States to prohibit the transfer of personal data to States that do not provide adequate levels of protection. The standard required by the OECD Guidelines and the Council of Europe Convention may be stronger as it is one of "equivalence" rather than "adequacy", but only under the EU Directive must the transfer of data be blocked if the standard is not met. Because of the EU's economic importance, the potential of such a data embargo is a powerful incentive for states around the world to create some measure of harmonization in the protection of personal data.[116] Where the transborder flow of data is interrupted because a third country has

II

[114] The EU Directive itself was negotiated under the threat of a data embargo from certain EU members with data protection laws, including France and Germany, against others with less stringent laws, such as Italy. Through the creation of similar data protection standards the possible interruption of the free flow of data was averted. Gregory Shaffer, "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards," (2000) 25(1) Yale Journal of International Law 1 at 10.

[115] For a discussion of the privacy protection regimes of OECD countries see: OECD; Directorate for Science, Technology, and Industry; Committee for Information, Computer and Communications Policy; Working Party on Information Security and Privacy; "Inventory of Instruments and Mechanisms Contributing to the Implementation and Enforcement of the OECD Privacy Guidelines on Global Networks," DSTI/ICCP/REG (98)12/FINAL, (19 May 1999).

[116] For example, the potential extra-territorial effects of the EU Directive have encouraged non-European countries such as Canada, Hongkong, New Zealand and Taiwan to pass data protection legislation to cover the private sector. See: Privacy Commissioner, New Zealand, "Report by the Privacy Commissioner to the Minister of Justice on the Trans-Tasman Mutual Recognition Bill and Transborder Data Flows," at Privacy Commissioner, New Zealand, "Reports and Submissions": <http://www.privacy.org.nz/people/transtas.html>.

inadequate privacy protection laws, the European Commission is required to enter into negotiations with that third country.

2. Safe harbour principles

In view of the entry into force of the EU Directive on 25 October 1998, the European Commission and the US Department of Commerce took up negotiations to avoid a disruption in the free flow of data between Europe and the United States. To diminish the

uncertainty as to whether US organizations would meet the “adequate standard” test with respect to data protection required by the EU Directive, the United States proposed that US companies that wish to receive personal data from European Union adhere to the so-called Safe harbour principles.[117] Adherence to these Principles would establish a “presumption of adequate privacy protection” for the purposes of the EU Directive.

Decisions by organization to qualify for the safe harbour are voluntary. Organizations may qualify for the safe harbour in several ways. They can join a self-regulatory privacy programme that adheres to the Principles or they can develop their own self-regulatory privacy policies, provided that they conform with the Principles. If an organization fails to comply with self-regulation, it can be pursued under Section 5 of the Federal trade commission act, which prohibits “unfair and deceptive acts”. Organizations which are subject to a statutory, regulatory, administrative or other law that effectively protects privacy may also qualify for the safe harbour. To qualify, organizations must self-certify to the Department of Commerce their adherence to the Principles in accordance with the guidance set forth in the Frequently asked questions.

The Safe harbour principles, issued in their final version on 21 July 2000, are the following:

"Personal data" and "personal information" are data about an identified or identifiable individual that are within the scope of the Directive, received by a U.S. organization from the European Union, and recorded in any form.

NOTICE: An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party(1).

CHOICE: An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party(1) or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

For sensitive information (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive.

ONWARD TRANSFER: To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is

II

[117] US Department of Commerce, “Safe Harbour Principles” (21 July 2000), online: Privacy Exchange, News: http://www.privacyexchange.org/.See also: online: Europa, European Commission, Internal Masrket, Media Information Society and Data Protection, Data Protection, News, <http://www.europa.eu.interamericano/comm/internal_market/en/media/dataprot/news/safeharbor.htm>

required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.

SECURITY: Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.
DATA INTEGRITY: Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.
ACCESS: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.
ENFORCEMENT: Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.
1. It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures.
These Principles are complemented by a document dealing with Frequently Asked Questions providing guidance to the interpretation of the Principles.[118]
Adherence to the Principles may be limited by the following:
a) to the extent necessary to meet national security, public interest, or law enforcement requirements;
b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or
c) if the effect of the Directive or member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts.
The European Union recognizes the US Federal Trade Commission and the US Department of Transportation “as being empowered to investigate complaints and to obtain relief against unfair or deceptive practices as well as redress for individuals in case of non-compliance with the Principles implemented in accordance with the Frequently asked questions.”[119]

II

[118] Online: Privacy Exchange, News: <http://www.privacyexchange.org/>.
[119] “Annex to the Safe Harbour Principles”, online: Privacy Exchange, News: <http://www.privacyexchange.org/>.

Although the European Commission had already accepted the “adequacy” of the Safe Harbour Principles[120], the European Parliament called for the imposition of additional requirements on 14 July 2000:[121]
- recognition of an individual right of appeal to an independent public body instructed to consider any appeal relating to an alleged violation of the principles;
- an obligation on participating firms to compensate for the damage, whether moral

or to property, suffered by those involved, in the event of violations of the principles, and an undertaking by the firms to cancel personal data obtained or processed in an unlawful manner;
- ease of identification of the steps to be taken to ensure data are cancelled and to obtain compensation for any damage suffered;
- provision of a preliminary check by the Commission on the proper functioning of the system within six months of its entry into force and presentation of a report on the outcome of the check and any problems encountered to the working party provided for in Article 29 and the Committee provided for in Article 31 of the Directive, as well as to the relevant committee of the European Parliament;

Despite these concerns by the European Parliament, the European Commission issued a Decision on 27 July 2000, accepting the Safe Harbour Principles released by the Government of the United States on 21 July 2000.[122] The Commission decided to proceed with the Decision, given that the European Parliament had not found that the Commission, in doing so, would be exceeding its powers. Nevertheless, the Commission notified the US Department of Commerce of the concerns of the European Parliament and stated that it would re-open discussions if Parliament's fears about the inadequacy of remedies for individuals proved to be well-founded.

3. Mutual assistance and cooperation

Where countries cannot agree on the establishment of a common data protection regime through the harmonization of laws or other mechanisms such as the *Safe harbour principles*, the effectiveness of national legislation can nevertheless be enhanced through mutual assistance and cooperation arrangements. In order to enforce data protection laws, adjudicative bodies must be able to exercise some control or influence over the offender and obtain the necessary evidence. Particularly in the area of personal data protection on the Internet and other global networks, international cooperation is required as individual countries alone cannot possibly deal with this issue. Some of the international instruments discussed above as well as national laws provide for cooperation among data protection authorities across international borders. Provisions for mutual assistance have also been included in other bilateral and multilateral treaties, particularly those dealing with criminal law.[123]

a) Mutual assistance in international instruments

The OECD Guidelines encourage members to exchange information related to the Guidelines and to facilitate "mutual assistance in the procedural and investigative matters involved."[124] The European Council Convention requires each Party's national data protection authority to provide information on its laws and administrative procedures in the field of data protection to other Parties and to assist persons resident abroad to exercise their rights.[125] The EU Directive stipulates that a national "authority may be requested to exercise its powers by an authority of another member State" and that "supervisory

[120] Commission Decision C5-0280/2000

[121] European Parliament Resolution on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce (C5-0280/2000 – 2000/2144 (COS)) in "Minutes of 05/07/2000 – Provisional Edition"on the web site of the European Union, European Parliament Search Guide, Resolutions; <http://www.europart.eu.interamericano/search/en/docsearch.htm#bresolutions>

[122] Data protection: Commission adopts decisions recognising adequacy of regimes in US, Switzerland and Hungary", online: Europa, European Commission, Internal Market, Media Information Society and Data Protection, Data Protection, News, <http://www.europa.eu.int/comm/internal_market/en/media/dataprot/news/safeharbor.htm>.

[123] See for example: *Treaty Between the Government of the United States and the Government of Canada on Mutual Legal Assistance in Criminal Matters* (18 March 1985) 24 I.L.M. 1092 and the *Canadian Mutual Legal Assistance in Criminal Matters Act*, ch. M-13.6 (R.S., 1985, c. 30 (4th Supp.); online: Canada, Department of Justice, "Consolidated Statutes" http://canada.justice.gc.ca/FTP/EN/Laws/Chp/M/M-13.6.txt.

[124] OECD Guidelines, Part V.

[125] European Council Convention, Articles 13 & 14.

authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information."[126]

b) Draft Convention on Cyber-Crime

Of relevance to the discussion of international data protection and mutual legal assistance is the proposed Convention on cyber-crime which is currently being negotiated by the member States of the Council of Europe and a number of other States, including Canada, Japan, South Africa and the United States. The Council of Europe has published

the current version of the Draft Convention (Draft No. 19) on the Internet.[127] Several of the provisions of the Draft Convention relate directly to the protection of personal data, such as those dealing with illegal access to computer systems (Article 2); the illegal interception of computer data (Article 3); the interference with computer data (Article 4) or a computer system (Article 5); or other computer related offences such as forgery (Article 7) or fraud (Article 8).

In addition, the Draft Convention contains language which may be useful in dealing with questions of jurisdiction and mutual legal assistance. The Convention addresses the issue of jurisdiction in Article 19:

1. Each Party shall take such legislative and other measures as may be necessary to establish jurisdiction over any offence ... when the offence is committed:

a. [in whole or in part] in its territory or on a ship, an aircraft, or a satellite flying its flag or registered in that Party;

b. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. ...

5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

The Draft Convention clearly encourages States to assert jurisdiction over offenders on their territory as well as their nationals, by way of consultation if required.

Article 20 of the Draft Convention outlines general principles relating to international co-operation:

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through application of relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and national laws, to the widest extent possible for the purposes of investigations and proceedings concerning criminal offences related to computer systems and data, or for the collection of electronic evidence of a criminal offence.

States are called upon to use any available legal means to pursue offenders.

Article 22 of the Draft Convention calls on Parties to provide for expedited mutual assistance for the purpose of enforcement:

1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations and proceedings concerning criminal offences related to computer systems and data, or for the collection of electronic evidence of a criminal offence.

2. For the purpose of providing cooperation under articles 24 - 29, each Party shall, in urgent circumstances, accept and respond to mutual assistance requests by expedited means of communications, including [voice], fax or e-mail, to the extent that such means provide appropriate levels of security and authentication, with formal confirmation to follow where required by the requested State.

The Draft Convention provides for mutual assistance procedures for cases where no mutual assistance treaty or arrangement is in place between the requesting and the

II

[126] EU Directive, Article 28.

[127] Council of Europe, Directorate General I, Legal Affairs, Treaty Office, *"Draft Treaties":* <http://conventions.coe.int/treaty/EN/cadreprojets.htm> [hereinafter Draft Convention on Cyber-crime].

requested Parties. Each Party is required to designate a central authority to deal with requests for mutual assistance. A register of central authorities is to be kept and the central authorities are to communicate directly with each other. Assistance may be refused, in full or in part, if required by law or if it would prejudice a Party's sovereignty, security, public order, or other essential interests. Parties may also forward to other Parties, without prior request, information which may lead to a request or to the initiation of an investigation. The information provided may only be used for specified purposes and may have to be kept confidential.[128] Requests for assistance may also concern the expedited preservation of data

stored on computers.[129] If a third State was involved in the transmission of a communication, a Party may request the disclosure of a sufficient amount of data, in order to identify the service provider and the path which was used for the communication.[130] When a Party requests to access, seize, secure or disclose data stored on computers, the requested Party should respond as expeditiously as possible by:

a) Where permitted by its domestic law, ratifying or endorsing any judicial or other legal authorisation that was granted in the requesting Party to search or seizure the data, thereupon executing the search or seizure and, pursuant to its mutual assistance treaties or laws, as applicable, disclosing any data seized to the requesting Party; or

b) Responding to the request and disclosing any data seized, pursuant to its mutual assistance treaties or laws, as applicable; or

c) Using any other method of assistance permitted by its domestic law.

In order to ensure immediate assistance in the form of technical advice, the preservation of data, or the collection of evidence, giving of legal information, and locating of suspects, a point of contact available on a 24 hour, 7 day per week basis needs to be established.[131]

While the Draft Convention on Cyber-Crime deals with criminal law matters, its mutual legal assistance provisions may nevertheless be of value to international efforts to protect personal data, particularly given the fact that the Convention deals with an area of law which is very closely related.

c) Cyber-Crime and G-8 Countries

A parallel process on the issue of cyber-crime is also under way under the auspices of the G-8 Countries. At the Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime on 19-20 October 1999, a statement on the principles on transborder access to stored computer data was released which also contains provisions for "expedited mutual legal assistance":[132][123]

4. Upon receiving a formal request for access, search, copying, seizure or disclosure of data, including data that has been preserved, the requested State shall, in accordance with its national law, execute the request as expeditiously as possible, by:

a. Responding pursuant to traditional legal assistance procedures; or

b. Ratifying or endorsing any judicial or other legal authorization that was granted in the requesting State and, pursuant to traditional legal assistance procedures, disclosing any data seized to the requesting State; or

c. Using any other method of assistance permitted by the law of the requested State.

5. Each State shall, in appropriate circumstances, accept and respond to legal assistance requests made under these Principles by expedited

[128] Draft Convention on Cyber-Crime, Article 23.
[129] Draft Convention on Cyber-Crime, Article 24.
[130] Draft Convention on Cyber-Crime, Article 25.
[131] Draft Convention on Cyber-Crime, Article 27.
[132] "Communique: Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime (Moscow, October 19-20,1999)", online: Canada. Department of Foreign Affairs and International Trade, <http://www.dfait-maeci.gc.ca/foreignp/g7/1999/moscow1-e.htm>.

but reliable means of communications, including voice, fax or e-mail, with written confirmation to follow where required.

Again, there is a recognition that effective mutual legal assistance is required in order to deal with data stored in a foreign State.

IV. CONCLUSION

The protection of personal information and data held in electronic form in the private sector has been advanced through the establishment of international instruments. The OECD Guidelines, the European Council Convention, the UN Guidelines, and particularly the EU Data Protection Directive have had a profound impact on data protection in Europe and elsewhere. Also some OAS countries, notably Canada and Chile, have enacted laws which provide relatively high levels of privacy protection.

Nevertheless, it seems fair to say that many challenges remain particularly with respect to the transborder flow of personal data on the Internet and other global networks. The privacy of citizens remains vulnerable even in those countries which have effective national laws, because of the existence of data havens where no protection is available. The existing international and national instruments leave numerous problems unresolved, such as the interpretation of what “adequate” and “equivalent” levels of protection are or the nature of the enforcement required to implement agreed upon standards. Legislation and enforcement are especially challenging because of rapidly evolving technology. In addition, those States who wish to protect the privacy of their citizens are also faced with competing economic, trade, social and political interests.

These difficulties, however, are not unique to the area of data protection. Further progress in the area of privacy protection could probably be made by a combination of measures, including the development of international standards and enforcement mechanisms, mutual legal and technical assistance, the encouragement of industry selfregulation, and the operation of market forces influenced by information and education.

Based on the limited information which was available for this report, however, it is difficult to assess the adequacy of legislation throughout the OAS. It is therefore recommended that, in order to obtain a more complete assessment of the juridical issues concerning personal data protection in OAS countries, the Secretariat for Legal Affairs repeat its request to member States for more information on existing domestic legislation, regulations, and policies.