Protection of personal data

CJI/doc.402/12 rev. 2

PROPOSED STATEMENT OF PRINCIPLES FOR PRIVACY AND PERSONAL DATA PROTECTION IN THE AMERICAS

(presented by Dr. David P. Stewart)

The OAS General Assembly, at its 41st meeting in San Salvador in 2011, directed the Inter-American Juridical Committee to "present, prior to the forty-second regular session, a document of principles for privacy and personal data protection in the Americas … with a view to exploring the possibility of a regional framework in the area." AG/RES. 2661 (XLI-O/11) (June 7, 2011).

In preparing these principles, the Committee has been instructed to take into account (i) the draft preliminary principles and recommendations on the protection of personal data which have been prepared by the Department of International Law (CP/CAJP-2921/10 rev. 1) and (ii) a comparative study of different existing legal regimes, policies and enforcement mechanisms for the protection of personal data which will be prepared by the Department of International Law.

At its 79th Regular Session in August 2011, the Committee gave initial consideration to this assignment on the basis of Preliminary Comments set forth in CJI/doc.382/11 (March 18, 2011). The Committee also named a Rapporteur for the purpose of preparing a set of proposed principles in response to the mandate of the General Assembly.

In the meantime, the Department of International Law has presented a document setting forth "Preliminary Principles and Recommendations on Data Protection (The Protection of Personal Data)," CP/CAJP-2921/10 rev. 1 corr. 1, 11 October 2011. On October 31, 2011, the Department circulated to all OAS member states a questionnaire on privacy and data protection in order to ascertain the current status of legislative developments and proposals in this field (CP/CAJP-3026/11). More recently, the Department has circulated a lengthy and detailed "annotated outline" of its "comparative study of different existing legal regimes, policies and enforcement mechanisms for the protection of personal data" (DDI/doc.03/12, 10 February 2012).

There can be no question the concept of privacy is well-established in international law or that it underpins the fundamental principles of personal honor and dignity as well as freedom of speech, opinion and association. Within our hemisphere, these principles are clearly established in the American Declaration of the Rights and Duties of Man (1948)[1/] as well as the American Convention on Human Rights ("Pact of San Jose").[2/] Provisions on privacy, protection of personal honor and dignity,

---

1. See Art. IV of the American Declaration of the Rights and Duties of Man.
2. See Arts. 11 and 13 of the American Convention on Human Rights.

freedom of expression and association, and the free flow of information are found in all the major human rights systems of the world.[3/]

These fundamental principles are increasingly challenged by the revolution in digital information and communication technology. We live today in a "global information economy." More information about individuals is collected, processed and made available faster than ever, by governments as well as private entities including commercial companies, journalists and members of the media, and even by non-commercial advocacy groups. In the face of these developments, it is more important than ever to take measures to protect the fundamental rights of individuals to privacy. At the same time, it must be recognized that the collection of personal data and information from and about individuals is often not just appropriate but necessary, and that many applications are entirely legitimate and lawful. It is also essential to recognize that in a rapidly globalizing economy, the free flow of information across borders remains a prerequisite for a free and vibrant economy; unnecessary restrictions can impose significant (and often unintended) non-tariff barriers to trade and development. While abuses do occur and must be addressed, excessive regulation and overly restrictive provisions can do more harm than good.

Throughout the world, national authorities are working to address these issues and, not surprisingly, they sometimes adopt differing approaches and apply competing values in inconsistent ways. Today, a majority of countries recognize a constitutional right of privacy, and many others provide additional privacy protections by statute or regulation, including in particular by imposing restrictions on the government and public agencies. More than 80 countries now have data protection and privacy laws extending beyond the public sector, and legislative efforts are under way in many others.[4/] But the specific provisions are by no means identical. The result is a diversity of national laws, rules and regulations reflecting divergent approaches in many important respects.[5/]

In addition, intensive efforts have been undertaken over the past several decades to adopt agreed principles at the regional and international level, in particular within the Organization for Economic Cooperation and Development (OECD), the Council of Europe (COE), the European Union (EU), and the Asia-Pacific Economic

---

3. See, e.g., the Universal Declaration of Human Rights (arts. 12, 18-20), the International Covenant on Civil and Political Rights (arts. 17-19), the European Convention on Human Rights and Fundamental Freedoms (arts. 8-10), the Charter of Fundamental Freedoms of the European Union (arts. 1, 7, 8, 10-12), and the African Charter of Human and Peoples' Rights (arts. 5, 8-11 and 28). Only the EU Charter specifically addresses privacy in the context of data protection. Art. 8 provides (1) that everyone has the right to the protection of personal data concerning him or her, (2) that such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law, and that everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified, and (3) compliance with these rules shall be subject to control by an independent authority.

4. Among others, they include Mexico, Uruguay, Peru, Colombia, Costa Rica, Canada and Brazil.

5. As noted in CP/CAJP-2921/10 rev. 1 corr. 1, "the meaning of privacy and the origins of an individual's right to privacy can vary. As a result, policies and laws governing the right to privacy differ from country to country. Because of this divergence in the treatment of the right to privacy, legislation protecting the treatment of personal data can vary between or even within regions."

Cooperation (APEC) forum.[6/] The most significant of these efforts were summarized in the previous report to the Committee (in CJI/doc.382/11, March 18, 2011). But the documents adopted by these various bodies are by no means identical and often differ both in detail and in basic approach.

A review of these varying national and regional approaches reveals both a measure of commonality but also significant divergences in principle as well as approach. For example, it does not appear that there is a single, commonly accepted definition of "personal" or "sensitive" information or "data protection," much less "privacy" itself. Nor is there a single, agreed upon concept of the "threat" or of the proper response to that threat. Some see the gathering and use of private information by the government and its agencies as the main threat and seek to constrain it, while others fear the private sector more and look to government oversight and regulation for protection.

Some seek to empower individuals, especially consumers, though an emphasis on consent, transparency, corporate "accountability" and "data stewardship," while others prefer direct government regulation of all "data collectors, managers and controllers." Some endeavor to address the issues through a single, comprehensive law, while others take a sectoral or topical approach providing varying levels of government oversight for different types of activities in different ways. Some advocate the individual's "right to be forgotten" or "right to oblivion" (including a right to the removal of all information even if accurate) while others propose a right to "rectification" or "remediation" (meaning a right to have errors and misstatements corrected).

It is evident that the issues are dynamic, the discussion remains active, and national as well as regional approaches continue to evolve. Which specific practices are acceptable, and which must be circumscribed or prohibited, is likely to depend on how one approaches the problem. The answers may differ when considered from a national security or law enforcement perspective, or as a matter of social regulation, or from the perspective of protecting technological innovation, promoting trade and development, protecting against foreign intrusion, etc. At the current time, it must be concluded that "one size does not fit all." An effort to describe or impose a single, detailed regulatory approach stands little chance of gaining widespread approval in the short run.

What is more likely to be acceptable, and what the OAS General Assembly appears to have requested, is a statement of general principles to guide further consideration of the issues. Towards that goal, the following principles (attached as

---

6. The EU will soon replace the scheme established by Directive 95/46 (Oct. 24, 1995) on the protection of individuals with regard to the processing of personal data, under which both the public and private sectors in member countries have been operating for thirteen years. Amendments announced on January 25, 2012 (to become effective after some years) promise a new EU "regulation" aimed at building a "digital single market" to replace the various national approaches to implementing the prior Directive. The new regulation will enshrine the "right to be forgotten," which has been the subject of considerable debate. Within the COE, the Grand Chamber of the European Court of Human Rights recently issued a significant ruling on privacy in Axel Springer v. Germany, App. No. 39954/08 (Feb. 7, 2012), holding that the rights of the publisher of the German tabloid "Bild" under art. 10 had been violated when it was prevented from publishing articles about the arrest and conviction of a well-known television actor for possession of cocaine.

Annex A) have been prepared on the basis of a review of emerging national law and practice, as well as the agreed (but differing) principles of the various regional and international groups which have addressed the problem to date.

In addition to the draft preliminary principles and recommendations on the protection of personal data which have been prepared by the Department of International Law (CP/CAJP-2921/10 rev. 1 corr. 1), and its "annotated outline" of a "comparative study of different existing legal regimes, policies and enforcement mechanisms for the protection of personal data" (DDI/doc.03/12), the Rapporteur considered the following international sources in the preparation of these proposed principles:

- The APEC Privacy Principles adopted as part of the APEC Privacy Framework and its 2011 Cross-Border Privacy Rules System

  http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx, and http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_010.pdf

- The 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

  http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

- The 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

  http://conventions.coe.int/treaty/en/treaties/html/108.htm

- 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, Official Journal L 281, 23/11/1995 P. 0031 – 0050

  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT

- Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation), Brussels, 25.1.2012, COM(2012) 11 final, 2012/0011 (COD)

  http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

- UN Guidelines for the Regulation of Computerized Personal Data Files, adopted by the UN General Assembly Resolution 45/90 (Dec. 14, 1990)

  http://www.un.org/documents/ga/res/45/a45r095.htm

While drawing in significant part from these earlier efforts (as well as from a variety of national laws), the attached principles are intentionally aimed at a level of generality which will permit their acceptance in national legal systems which are at different stages in their consideration of the issues and which may have different

orientations and priorities. They also reflect the fact that the OAS as a regional organization differs in many respects from the European Union and the Council of Europe, as well as from APEC and the OECD. The proposed principles are intended to establish a broadly acceptable base-line for further development, rather than to impose any one particular model or approach to be directly implemented by all OAS member states.

Annex A

PROPOSED STATEMENT OF PRINCIPLES FOR PRIVACY AND PERSONAL DATA PROTECTION IN THE AMERICAS

Introduction

The following list sets forth the basic principles which should be adopted and followed in national law and practice. They are intended to prevent harm to individuals from the wrongful or unnecessary collection or use of personal data and information. The twelve principles are interrelated and should be interpreted together as whole. In addition, each national system should adopt a clear and effective policy of openness and transparency about all developments, practices and policies with respect to personal data and information. In this context, the Inter-American Juridical Committee proposes to the General Assembly of the Organization of American States the adoption of the following principles.

First principle: Lawful and Fair Purposes

Personal data and information should be collected only for lawful purposes and by fair and lawful means.

Second Principle: Clarity and Consent

The purposes for which personal data and information are collected should be specified at the time the information is collected. As a general rule, personal data and information should only be collected with the knowledge or consent of the individual concerned.

Third Principle: Relevant and Necessary

The data and information should be accurate, relevant and necessary to the stated purposes for which they are collected.

Fourth Principle: Limited Use and Retention

Personal data and information should be kept and used only in a lawful manner not incompatible with the purpose(s) for which it was collected. It should not be kept for longer than necessary for that purpose or purposes and in accordance with relevant domestic law.

Fifth Principle: Duty of Confidentiality

Personal data and information should not be disclosed, made available or used for purposes other than those for which it was collected except with the consent of the concerned individual or under the authority of law.

Sixth principle: Protection and Security

Personal data and information should be protected by reasonable and appropriate security safeguards against unauthorized access, loss, destruction, use, modification or disclosure.

Seventh Principle: Accuracy of Information

Personal data and information should be kept accurate and up-to-date to the extent necessary for the purposes of use.

Eighth Principle: Access and Correction

Reasonable methods should be available to permit individuals whose information has been collected to seek access to that information and to request that the record keeper amend, correct or delete that information. If such access or correction needs to be restricted, the specific grounds for any such restrictions should be specified in accordance with domestic law.

Ninth Principle: Sensitive Information

Some types of information, given their sensitivity and in particular contexts, are especially likely to cause material harm to individuals if misused. Record keepers should adopt privacy and security measures that are commensurate with the sensitivity of the data and its capacity to harm individual data subjects.

Tenth Principle: Accountability

Record keepers should adopt appropriate procedures to demonstrate their accountability for their compliance with these principles.

Eleventh Principle: Trans-border Flow of Information and Accountability

Member states should cooperate with one another in developing mechanisms and procedures to ensure that record keepers operating in more than one jurisdiction can be effectively held accountable for their adherence to these principles.

Twelfth Principle: Disclosing Exceptions

When national authorities make exceptions to these principles for reasons relating to national sovereignty, internal or external security, the fight against criminality, regulatory compliance or other public order policies, they should make those exceptions known to the public.

* * *