CJI/doc.382/11

PRELIMINARY COMMENTS ON A STATEMENT OF PRINCIPLES FOR PRIVACY AND PERSONAL DATA PROTECTION IN THE AMERICAS

(presented by Dr. David P. Stewart)

At its recent 41st meeting in San Salvador, the OAS General Assembly 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 this document, the Juridical Committee is 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.

The Inter-American Juridical Committee initially considered this topic as part of its work on "Access to and Protection of Information and Personal Data in Electronic Format," in response to the OAS General Assembly's directive in AG/RES. 2288 (XXXVII-O/07).[1] In adopting the Principles on the Right of Access to Information,[2] however, the Juridical Committee did not focus specifically on issues related the right to privacy and the need to protect personal data. It is now time for the Committee to turn its attention to these important issues.

No one disputes the importance of protecting personal data in a world of rapidly expanding information technology. The concept of privacy underpins the fundamental principles of human dignity as well as freedom of speech, opinion and association. These principles are clearly established in the American Declaration of the Rights and Duties of Man (1948)[3] as well as the American Convention on Human Rights ("Pact of San Jose").[4] Similar provisions are found in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the European Convention on Human Rights. At the same time, it is essential to protect the free flow of information across borders. That, in turn, protects and promotes freedom of trade and commerce, upon which economic progress and development depends.

However, as all members of the Committee recognize, global communications technologies and media practices pose increasingly serious challenges to those fundamental notions of privacy, data protection, and reputation, as well as to the critical need to protect and promote freedom of speech and the press and the free flow of information across borders. The growing sophistication of digital information technology enables private entities as well as governments to collect, analyze and disseminate much more personal information, more quickly, that ever before. In addition, new

---

1 AG/RES. 2607 (XL-O/10) adopting the proposed Model Inter-American Law on Access to Public Information, June 8, 2010. See also AG/RES. 2514 (XXXIX-O/09), adopted June 4, 2009.

2 See "Principles on the Right of Access to Information," CJI/RES. 147 (LXXIII-O/08), adopted August 7, 2008.

3 The American Declaration of the Rights and Duties of Man provides in Art. IV that "[e]very person has the right to freedom of investigation, of opinion, and of the expression and dissemination of ideas, by any medium whatsoever" and in Art. V that "[e]very person has the right to the protection of the law against abusive attacks upon his honor, his reputation, and his private and family life."

4 The American Convention on Human Rights states in Art. 11 that: 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, and 3. Everyone has the right to the protection of the law against such interference or attacks. Article 13 of the American Convention on Human Rights guarantees: 1. Everyone has the right to freedom of thought and expression. This right includes freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice.

developments in medical research and care, telecommunications, advanced transportation systems and financial transfers have dramatically increased the level of information generated by each individual. Computers linked together by high speed networks with advanced processing systems can create comprehensive dossiers on any person anywhere, without the need for a single central computer system.

Applications involving these new technologies include identity cards, biometrics (e.g., digitized photographs, retina scans, hand geometry, voice recognition, DNA identification, communications surveillance, Internet and email interception, video surveillance (closed circuit television), and so forth. These technologies are increasingly available not only to governments but also to the private sector, including commercial companies, journalists and members of the media, and even non-commercial advocacy groups. Many applications are entirely legitimate and lawful. For example, commercial enterprises collect, store and disseminate personal information on customers and consumers; some routinely collect information from email and internet usage for marketing purposes. Unfortunately, it is not uncommon for them to be used for improper or even illegal purposes, such as to non-consensual monitoring of the communications, activities and locations of public and private persons, political opponents, human rights workers, journalists and labor organizers, and economic competitors.

Today, a majority of countries recognize a right of privacy explicitly in their Constitutions. At a minimum, these provisions include rights of inviolability of the home and confidentiality of communications. Many national constitutions (such as those in South Africa and Hungary) guarantee specific rights to access and control one's personal information. In many other countries where privacy is not explicitly recognized in the national constitution (such as the United States, Ireland and India), the courts have found that right in various provisions of law. In others, international agreements that recognize privacy rights have been adopted and implemented by legislation.

Throughout the world, a general movement is pressing for the adoption of more specific domestic privacy laws that set national legal frameworks for the protection of individual data. Within the OAS, the effort is starting to gather momentum. To date, a few states (including, for example, Mexico, Peru, Costa Rica, Canada and Brazil) have recently adopted or are actively working on new privacy legislation. However, no regional model or coordinated approach currently exists for addressing these issues at the national level. Neither the Inter-American Court of Human Rights nor the Inter-American Commission of Human Rights appears have given significant attention to the issues.[5]

The Committee thus has the opportunity to make a significant contribution to this field. In doing so, it should of course take into account efforts which have been undertaken in other regions as well as the extensive studies on data privacy which are taking place in the Organization for Economic Cooperation and Development, in Europe (in the Council of Europe as well as the European Union), in the Asia-Pacific Economic Forum, and elsewhere.

OECD. In 1980, the Organization for Economic Cooperation and Development adopted non-binding, technologically-neutral principles for possible use in establishing either a legal framework or an industry standard. The eight "Guidelines Governing the Protection of Privacy and Trans-border Data Flows of Personal Data" apply to both governmental and commercial uses of personal data. They call for (1) limiting the collection of personal data and ensuring that such information should only be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject; (2) ensuring that the information collected should relevant to the purposes for which they are to be used, accurate, complete and up-to-date; (3) specifying the purposes for which personal data are collected; (4) not disclosing or using data for purposes other than those specified in advance; (5) protecting the data by reasonable security safeguards; (6)

---

[5] See the Commission's Report on Terrorism and Human Rights (paras. 280-95 discussing *habeas data*). See also the recent Report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (Frank La Rue), UN doc. A/HRC/17/27 (May 16, 2011), at para. 59 ("there are insufficient or inadequate data protection laws in many States stipulating who is allowed to access personal data, what it can be used for, how it should be stored, and for how long.")

establishing a general policy of openness about developments, practices and policies with respect to personal data; (7) giving individuals the right to obtain personal data within a reasonable time and in a reasonable manner; and (8) holding data controllers accountable for complying with the requirements of these principles.

Europe. The approach of European countries to the issues of privacy and data protection has largely been based on a combination of national laws, the 1981 Council of Europe Convention for the Protection of Individuals with Regard for Automatic Processing of Personal Data (ETS No. 108), the 1950 European Convention on Human Rights and Fundamental Freedoms and the 2007 Charter of Fundamental Rights of the European Union, and a series of EU directives and regulations.

The EU itself first adopted a rule of data protection in 1995, requiring each EU member State to adopt conforming legislation.[6] At the time, the EU Data Directive could only govern the private sector because the EU's powers were limited (before the Lisbon Treaty). It has since been supplemented by an EU E-Privacy Directive.[7] Generally speaking, these directives require that data must be processed fairly and lawfully, collected for specific and legitimate purposes, be adequate and relevant for those purposes, accurate and kept up to date, and retained no longer than necessary. In addition, a Telecommunications Directive now establishes specific protections covering telephone, digital television, mobile networks and other telecommunications systems.[8] The Telecommunications Directive imposes wide scale obligations on carriers and service providers to ensure the privacy of users' communications. Access to billing data will be severely restricted, as will marketing activity. Caller ID technology must incorporate an option for per-line blocking of number transmission. Information collected in the delivery of a communication must be destroyed once the call is completed.

Every EU country has a "privacy commissioner" or agency to enforce the rules,[9] and it is expected that foreign countries with which EU members do business will adopt a conforming level of oversight. In other words, the Directives aim to guarantee that the rights of European data subjects follow their data to other countries. Thus, the Directives prohibit data export to non-EU countries that lack an "adequate level" of data protection as determined by the European Commission. As a result, companies operating within the EU are not allowed to send personal data to countries outside the EU unless those countries can guarantee that the data will receive levels of protection equivalent to the EU requirements. This restriction pressures other countries to conform to European standards. Countries (and companies) refusing to adopt meaningful privacy laws may find themselves unable to conduct certain types of information flows with Europe, particularly if they involve sensitive data.

United States. In the United States, the federal Constitution has been interpreted to include a right of privacy,[10] and various federal privacy statutes address data protection and privacy issues in specific contexts or sectors of activity, such as credit reports (Federal Credit Reporting Act of 1970), health data (the Health Information Portability and Accountability Act of 1996), the federal government's collection of personal data (the Privacy Act of 1974, the e-Government Act of 2002,

---

[6] Directive 95/46, Oct. 24, 1995) on the protection of Individuals with regard to the processing of personal data amended by Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and on the free movement of such data.

[7] Directive 2002/58 (July 12, 2002), amended in 2006 and more recently by Directive 2009/136 (Nov. 25, 2009) and services. See also Directive 2002/58/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector, and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

[8] Directive 2006/24 ((March 15, 2006) on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks. Other relevant European instruments include the 1981 Council of Europe Convention for the Protection of Individuals with Regard for Automatic Processing of Personal Data (ETS No. 108).

[9] See, e.g., Regulation (EC) No. 1211/2009 of the European Parliament and of the Council of November 25, 2009, establishing the Body of European Regulators for Electronic Communications (BEREC).

[10] Among the relevant decisions are Olmstead v. United States, 277 U.S. 438 (1928) (Justice Brandeis, dissenting); Griswold v. Connecticut, 381 U.S. 479 (1965); and Loving v. Virginia, 388 U.S. 1 (1967).

the Tax Confidentiality Act), etc. Other areas of commercial activity are actively regulated at the state (and sometimes local) levels. Not all private sector activity is necessarily subject to privacy regulation, and unlike the EU and its member states, there is no single omnibus or general purpose data protection law. However, new legislation is actively being considered at both the federal level (this spring, Senators Kerry and McCain introduced the Commercial Privacy Bill of Rights 2011) as well as in various states (including Vermont, Massachusetts, Illinois, and California).

The difference between the U.S. approach to commercial privacy and the 1995 EU Data Protection Directive was bridged by the so-called "Safe Harbor" framework adopted by the U.S, and the EU jointly in the late 1990s. The Safe Harbor framework is an innovative transnational arrangement designed to preserve free flow of information and trade. It allows certain U.S. companies to self-certify that they follow the Safe Harbor Privacy Principles, thus meeting the standards of EU privacy regulations. As a result, the EU will permit transfer of personal data to recipients who have adhered to the Safe Harbor principles and are subject to the enforcement authorities of either the U.S. Federal Trade Commission or the U.S. Department of Transportation.

The Safe Harbor principles require companies to provide seven particular guarantees: (1) notice - individuals must be informed that their data is being collected and about how it will be used; (2) choice - individuals must have the ability to opt out of the collection and forward transfer of the data to third parties; (3) "onward transfer" - transfers of data to third parties may only occur to other organizations that follow adequate data protection principles; (4) security - reasonable efforts must be made to prevent loss of collected information; (5) "data integrity" - data must be relevant and reliable for the purpose it was collected for; (6) access - Individuals must be able to access information held about them, and correct or delete it if it is inaccurate; and (7) enforcement - there must be effective means of enforcing these rules. Organizations adopting these principles must re-certify their compliance every 12 months, either through self-assessment or by a third-party. Appropriate employee training and dispute settlement mechanisms must be provided.

APEC. Still a different approach is being pursued by the Pacific Rim countries within the Asia-Pacific Economic Cooperation (APEC) forum, which, rather than pursuing harmonization of domestic privacy laws, has focused more specifically on the issue of trans-border transfers of personal data. For several years APEC has been working on a privacy initiative. A Framework with Privacy Principles was adopted in 2004, and an implementation program was added in 2005 to encourage domestic implementation of the Principles by individual member states. A Data Privacy Sub-group has been working to develop Cross Border Privacy Rules (CBPR) allowing businesses to be certified for transfer of personal information between participating APEC economies. A Cross Border Privacy Enforcement Cooperation Arrangement (CPEA) was established in 2010 to provide mutual recognition between participating APEC economies of each other's mechanisms for certification of a business's privacy rules. (The OECD has a similar enforcement network called GPEN.)

There is a certain measure of commonality in the principles adopted by these various groups. At a minimum, all require that personal information must be obtained fairly and lawfully; used in ways that are compatible with the original specified purpose; accurate, relevant and proportional with respect to purpose; accurate and up to date; limited in distribution to others; and destroyed after its purpose is completed. At the same, there are some significant differences in approach as well, including whether, when and how to apply the same principles to governmental entities, public service providers, private commercial enterprises, and even individuals; issues of criminal law enforcement and national security; as opposed to organizations,

The document prepared by the Department of International Law (CP/CAJP-2921/10 rev. 1) sets forth a series of fairly detailed draft principles entitled: Lawfulness and Fairness; Specific Purpose; Limited and Necessary; Transparency; Accountability; Conditions for Processing Disclosures to Data Processor; International Transfers; Individual's Right of Access; Individual's Right to Correct and Delete Personal Data; Right to Object to the Processing of Personal Data; Standing to Exercise Personal Data Processing Rights; Security Measures to Protect Personal Data; Duty of Confidentiality, and Monitoring, Compliance, and Liability.

The task of the Committee will be to review these proposals carefully, in light of the efforts of other groups and entities, and with an eye to the specific legal culture and needs of the OAS membership and region. Among the issues to be considered are the scope of application (private parties as well as government organs), the effect on national security and law enforcement interests, the requirement (rather than option) to have a central supervisory authority, the impact on existing (and developing) laws and practices at the national level), the relationship of restrictive principles on transborder flow of information and on free trade, and the need for exceptions or derogations as appropriate to the circumstances.

The threat to privacy is now greater than at any time in recent history. The power, capacity and speed of information technology are accelerating rapidly, and with it the extent of privacy invasion. Globalization has removed geographical limitations to the flow of data. There is a need for clear and effective principles to provide adequate protection of privacy without unduly hindering other important interests. That is the task in which the Committee has now been asked to participate.

REFERENCES

KNIGHT, S. “Regulatory Conflict over Data Privacy: Can the US-EU Safe Harbor Arrangement Be Sustained?” (American Consortium on European Union Studies, 2003)

SHAFFER, G. “Extraterritoriality in a Globalizing World: Regulation of Date Privacy,” 97 Am. J. Int’l L. 314, 2003.

KENYON, A. and RICHARDSON, M. (eds.). New Dimensions in Privacy Law: International and Comparative Perspectives. Cambridge, 2006.

LEVMORE, S. and NUSSBAUM, M. (eds.). The Offensive Internet: Privacy, Speech and Reputation. Harvard, 2010.

NOORDA, C. and HANLOSER, S. (eds.). E-Discovery and Data Privacy: A Practical Guide. Kluwer, 2011.

\