84rd REGULAR SESSION
March 10-14, 2014
Rio de Janeiro, Brazil

OEA/Ser.Q
CJI/doc. 450/14
February 25, 2014
Original: English
* Limited

PRIVACY AND DATA PROTECTION

(presented by Dr. David P. Stewart)

At the forty-third regular session of the OAS General Assembly (La Antigua, Guatemala, June 2013), the OAS General Assembly adopted Resolution AG/RES. 2811 (XLIII-O/13) instructing the Inter-American Juridical Committee "to prepare proposals for the Committee on Juridical and Political Affairs on the different ways in which the protection of personal data can be regulated, including a model law on personal data protection, taking into account international standards in that area.".

At the 83rd regular session of the Inter-American Juridical Committee (Rio de Janeiro, Brazil, August 2013) the Chairman requested Dr. David P. Stewart to serve as the rapporteur for the topic. Dr. Hyacinth Lindsay asked to work with the rapporteur on this topic.

The point of departure for this project is the Proposed Statement of Principles and Personal Data Protection in the Americans, adopted by the Committee at its 80th Regular Session in Mexico City in CJI/RES. 186 (LXXX-O/12) (March 2012) (see also the analysis in the accompanying report in CJI/doc.402/12 rev. 2). These principles aimed at encouraging Member States of the Organization to adopt measures ensuring respect for people's privacy, reputations, and dignity. They were intended to provide the basis for Member States to consider formulating and adopting legislation to protect the personal information and privacy interests of individuals throughout our hemisphere.

In light of the General Assembly's subsequent instruction in Resolution AG/RES. 2811 (XLIII-O/13, the most appropriate next step appears to be an elaboration of those principles with an eye to their acceptance and implementation by Member States, including the possibility of "a model law on personal data protection," taking into account relevant international standards and developments.

For that purpose, the rapporteur has been actively consulting over the past months with experts and others involved in the development of relevant principles and practices, including within the European Union and other regional groups, as well as with representatives from governmental, academic, corporate and non-governmental institutions. In late February, the rapporteur participated (together with Department of International Law Director Dante Negro and Senior Legal Officer Magaly McLean, in a very useful meeting organized in La Antigua, Guatemala by the Iberoamerican Network For Data Protection. Information has also been requested from Member States of the Organization about their current practices and laws in the area.

In the rapporteur's view, the response to the Committee's proposed Principles has been broadly favorable. In no case has the response been that the Principles contain any fundamental errors or even serious flaws. Most of the comments have either been (1) that more explanation and context is necessary or (2) that the Principles are not precisely the same as the particular guidelines or formulae adopted in other contexts.

As a result of these consultations, the rapporteur believes that the most appropriate direction for this project, at least for the next phase, is the preparation of a proposed legislative guide for Member States. This legislative guide should be based primarily on the 12 principles previously adopted by the Committee, taking appropriate notice and account of the various other sets of guidance prepared within the EU, the OECD, APEC, etc. In substance, the effort should be to expand upon those principles by giving additional context and guidance to Member States to assist in their preparation of national legislation. In this way, the focus will remain on principles and practices, taking into account of others in the field, rather than trying to agree on the precise details of exact legislative language.

In the rapporteur's view, the field of personal privacy and data protection continues to be characterized by rapid technological developments as well as constantly evolving threats to personal privacy. Moreover, different responses to these developments and threats have been adopted in different regions of the world. Within our hemisphere, a coherent "regional" approach does not seem to have emerged. In attempting to elaborate upon the principles, the Committee will be able to draw on the achievements in other regions while taking into account developments in our own hemisphere, in order to formulate a proposed framework for the American States to use in addressing this critical area. Put simply, it seems premature at this point to spend time drafting statutes or code provisions. More interaction with Member States is needed.

One possibly useful outcome would be a volume for distribution to Member States (governments, legislatures, experts, etc.) that includes (i) the OAS Principles on Privacy and Data Protection, (ii) an elaboration of the issues addresses by those Principles, and considerations to be taken into account in enacting them into domestic law, (iii) a compilation of relevant instruments from around the world (including for example the EU's General Data Protection Directive, the Madrid Principles, the OECD Privacy Guidelines, APEC's Privacy Framework, and various national legislation and "codes of conduct," etc.). If the text of a possible model law can in fact be elaborated, it too could be included.

By way of illustrating what an "elaboration of the principles" might entail, the attachment to this report includes a first draft of such a discussion for the first four principles. Comments on the approach reflected in that attachment are welcomed.

Attachment A

Internal Draft 2.24.14
Inter-American Juridical Committee

OAS PRINCIPLES ON PRIVACY AND DATA PROTECTION

The following elaboration of the OAS Principles on Privacy and Data Protection is intended to provide a guide to the preparation and implementation of national legislation and related practice within OAS member states. The fundamental purpose of the Principles is to establish a framework for guaranteeing the fundamental rights of the individual to personal data protection and informational self-determination. They are intended in particular to protect individuals from wrongful or unnecessary collection, use or retention of personal data and information.

The Principles are based on internationally recognized principles. They are interrelated and should be interpreted together as whole. In addition, each OAS Member State should adopt a clear and effective policy of openness and transparency about all developments, practices and policies with respect to personal data and information.

National legislation must establish effective rules for personal data protection that give effect to the individual's right to privacy and that demonstrate respect for their personal information. Personal information may only be collected for lawful purposes, and it must be processes in a fair, lawful and non-discriminatory manner. In particular, these rules must be aimed at ensuring that individuals receive the necessary information about the persons or entities collecting the information, the purpose for which the information is collected, the protections that are afforded to individuals, and the ways in which individuals can exercise those rights.

At the same time national legislation must protect the right of individuals to benefit from the digital economy and the information flows that support it. It must balance the right of individuals to control how their personal data is collected, stored and used with the interests of organizations in using personal data for legitimate and reasonable business purposes. Privacy legislation should allow consumers and companies to benefit from the use of personal data in a secure and protected manner. It must be balanced, technology-neutral, and permit the free flow of information within each country and across national boundaries in a way that fosters innovation and the growth of commerce.

In addition to (1) effective protection of privacy and (2) promoting free flow of information and economic progress, states must also follow (3) a general policy of transparency in respect of their policies and procedures. States may provide additional protections for the privacy of personal data.

Scope

These principles apply equally to the public and private sectors – that is, to personal data generated, collected or administered by government entities as well as to information gathered and processed by private entities. They apply to personal data contained in hard copy as well as electronic files. They do not apply to personal data used by an individual exclusively in the context of his or her private life.

Definitions

Personal Data. The term "personal data" is intended to include any information about an "identified individual." An identified individual is a natural person who has been or can be identified, whether directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. This definition recognizes that in many circumstances information can be collected or processed in a manner which does not identify any particular individual.

The Principles intentionally use both "data" and "information" in an effort to provide the broadest protection to the rights of the individuals concerned.

For purposes of these Principles, only people (natural persons) have privacy interests, not the devices,

computers or systems by which they interact. Neither do the organizations or other legal entities with which they deal. Minors (individuals below the age of adulthood) also have legitimate privacy interests which should be recognized and effectively protected by national law.

Sensitive Personal Data. The term "sensitive personal data" includes data affecting the most intimate aspects of natural persons, for example including (but not limited to) information related to an individual's personal health or sexual preferences, religious or philosophical beliefs, political opinions, or racial or ethnic origins. This data is considered "sensitive" and worthy of special protection because, if mishandled or improperly disclosed, it is particularly likely to lead to serious harm to the individual or to unlawful or arbitrary discrimination.

Data Subject. This term refers to the individual whose personal data is being collected, stored, used or disseminated.

Record Keepers. [tbd]

Authorities. [tbd]

OAS PRIVACY PRINCIPLES WITH ANNOTATIONS

FIRST PRINCIPLE: LAWFUL AND FAIR PURPOSES

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

This principle comprises two elements: (i) the "lawful purposes" for which personal data and information are initially collected and (ii) the "fair and lawful means" by which initial collection takes place.

The premise is that many if not most intrusions on the rights of individuals can be avoided if respect is given to the related principles of lawfulness and fairness at the outset, when data is initially collected. These principles of course apply and must be respected throughout the process of gathering, compiling, storing, using, disclosing and disposing of personal data -- not just at the point of collection. Yet they are more likely to be honored and respected if they are emphasized from the very beginning.

Lawful Purposes

The requirement of lawfulness in the purpose for which personal data is collected is a fundamental norm, deeply rooted in basic democratic values and the rule of law. Article 11 of the American Convention on Human Rights, for example, provides that "[n]o 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." See also article 17 of the International Covenant on Civil and Political Rights. Article 5 of the Council of Europe's 1981 Convention 108 on the Automated Processing of Personal Data requires all states party to ensure that "personal data undergoing automatic processing shall be...obtained and processed fairly and lawfully." The OECD Guidelines Governing the Protection of Privacy and Trans-border Flows of Data and the APEC Privacy Principles likewise contain a "Collection Limitation Principle" providing *inter alia* that data collection "should be obtained by lawful and fair means."

The requirement of lawfulness also excludes the arbitrary and capricious collection of personal data. It implies transparency and a legal structure that is accessible to the person whose data is being collected.

In many contexts, the lawfulness requirement could be enforced by requiring the record keeper to provide the data subject with the legal basis on which the data is being requested at the time of collection (e.g., "Your personal identification number is requested pursuant to the National Registration Law of 2004" or "Ministry of Economy Directive 33-25," etc.). In other situations, a different explanation may be required, such as "This information is required in order to guarantee that the refund of money is sent to the correct address of the claimant...".

Fair and Lawful Means

The First Principle also requires that the means by which the personal data is collected must be both "fair and lawful." Personal information is collected by fair and lawful means when the collection is consistent with *both* the applicable legal requirements and the reasonable expectations of individuals based on their relationship with the record keeper collecting the information and the notice(s) provided to individuals at the time their information is collected.

This principle excludes obtaining personal information by means of fraud, deception or under false pretenses. It would be violated, for example, when an organization misrepresents itself as another entity in telemarketing calls, print advertising, or email in order to deceive consumers and induce them to disclose their credit card numbers, bank account information or other sensitive personal information.

"Fairness" is of course contextual and depends on the circumstances. It requires, among other things, that individuals should be provided appropriate choices about how and when they provide personal information to record keepers when collection would not be reasonably expected given their relationships with the record keeper and the notice(s) they were provided at the time their information was collected. The choices provided to individuals should not interfere with record keepers' efforts and obligations to promote safety, security, and legal compliance, or otherwise prevent record keepers from engaging in commonly accepted practices regarding the collection and use of personal information.

In implementing these principles, Member States may decide to contain a separate "fairness" requirement that is distinct from the issue of deception.

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.

This principle also focuses on the collection of data and information. It comprises two principles which are widely recognized internationally: the "transparency" principle and the principle of "consent." Together, they require that (i) the purposes for which personal data are collected should be specified, (ii) such specification must be made not later that the point at which collection begins, and (iii) personal data and information should only be collected with the knowledge or consent of the individual concerned.

In addition to the types or categories of personal information to be collected, individuals should be informed about how that information may be used, whether and for what purposes it might be shared with third parties, and what measures are in place to assure its accuracy.

Clarity

The purposes for which personal data and information are collected must be clearly specified. In addition, individuals must be informed about the practices and policies of the entities or persons collecting the personal information so they can make an informed decision about providing the information. The requirement of clarity reinforces the general rule that information should only be collected with the knowledge or consent of the individual concerned. Without clarity, consent cannot be meaningful.

Accordingly, those responsible for collecting personal data must inform the individuals concerned at a minimum about the use to which they will put their personal data. In order for the data subjects to make an informed decision as to whom and for what reason they will provide their personal data, more information is needed than just the purposes of the handling of those data.

It is therefore important for the those individuals also be informed about how their personal data will be stored and processed, including the identity and contact information of the personal responsible for handling them, any data transfers that may be involved, and the means at their disposal for exercising their rights in respect of their personal information.

Consent

The individual must consent to the collection of personal data and in the manner and for the purposes intended. The individual's consent must be based on sufficient information and should be clear, that is, leaving no doubt or ambiguity about the individual's intent. For consent to be valid, the individual must have the ability to exercise a real choice and there must be no risk of deception, intimidation, coercion or significant negative consequences from refusal to consent. Consent should cover the specific details of the information to be collected, the purposes of the processing, and any disclosures that may be made.

The method of obtaining consent should appropriate to the age and capacity of the individual concerned and to the particular circumstances of the case. Clearly, consent obtained under duress or on the basis of misleading information does not adequately satisfy the condition for processing.

As a general rule, consent must be explicit. However, the Principles recognize that in some circumstances, "knowledge" may be the appropriate standard where data processing and disclosure satisfy legitimate interests. Individuals' knowledge or consent to the collection of their personal information may be inferred based on their interactions with record keepers, the notices provided by record keepers, commonly accepted practices regarding the collection and use of personal information, and record keepers' legal obligations. Implicit consent may be appropriate in limited circumstances but *never* in respect of sensitive personal data.

In any event, the party seeking to collect and process the information must show that it has a clear need to do so for the purposes of its legitimate interests or for those of a third party to whom the data may be disclosed. It must also demonstrate that the legitimate interests of the party seeking disclosure are balanced against the interest of the data subject concerned. The "legitimate interests" condition will not be met if the processing will have a prejudicial effect on the rights and freedoms, or legitimate interests, of the data subject.

Where there is a serious mismatch between competing interests, the subject's legitimate interests will come first. Finally, the processing of information under the legitimate interests condition must be fair and lawful and must comply with all the data protection principles. Sensitive personal data may only be processed without the subject's consent where it is in the substantial public interest.

Timing

The individuals must be informed of the purposes for which the information is being collected, and his or consent must be obtained, not later than the point at which the data is collected. In most cases, the purposes should be clearly stated prior to the eliciting of personal data so that the individuals in question can make an informed decision about providing the information.

In most cases, consent will last for as long as the processing to which it relates continues.

An individual is entitled to withdraw consent depending on the nature of the consent given and the purposes for which the information is collected. In general, withdrawal of consent does not affect the validity of anything already done on the basis of the consent.

THIRD PRINCIPLE: RELEVANT AND NECESSARY

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

Accuracy, relevancy and necessity are critical principles in respect of data protection and personal privacy. Of course, their requirements must be assessed in relation to the specific context in which the data and information are collected, used, and disclosed. Contextual considerations include what particular information is collected and the purposes for which it is collected.

Accuracy

Data collected from individuals should be kept accurate, complete and up-to-date with respect to the purposes for which it was collected. Inaccurate data can cause harm to both the record keeper and the data subject, but to an extent that varies greatly depending on context. The data collector should therefore adopt mechanisms to ensure that the personal data he or she handles are correct, accurate, complete, and up-to-date.

The data may or may not need to be continually updated and/or complete in order to be accurate in relation to the stated purpose for which the data was collected. In the APEC Privacy Principles, the Principle of Integrity of Personal Information requires that data collectors keep data "accurate, complete and kept up-to-date *to the extent necessary for the purposes of use*." Similarly, Article 5d of Convention 108 requires that data be kept "accurate, and *where necessary*, kept up to date." The OECD Principles contain virtually identical concepts in the Data Quality Principle.

Relevance

The requirement that data be "relevant" means, essentially, that data must be reasonably related to the purposes for which it was collected and is intended to be used. For instance, data concerning opinions may easily be misleading if they are used for purposes to which they bear no relation.

Necessity

Personal data and information should only be collected and used to fulfill the purposes for which they were collected, for example when necessary to provide the service or product that was requested by the individual. They should be commensurate with, and not exceed, the stated purposes of collection. They should follow a "minimization" criterion, according to which the person responsible for collection should make a reasonable effort to ensure that the personal data handled correspond to the minimum required for the stated purpose.

Proportionality

In some legal systems the concept of "proportionality" is used to refer generally to the balancing of competing values. Proportionality enables decision-makers to decide whether a measure has gone beyond what is required to attain a legitimate goal and whether its claimed benefits will exceed the anticipated costs. In the context of public sector data processing, the idea of necessity is sometimes measured by proportionality, for example to require balancing (i) the public interest in processing the personal data against (ii) protection of the individuals' privacy interests.

In the APEC Privacy Framework (which, by contrast, deals exclusively with commercial record keepers) the term "necessary" places limitations on use rather than collection, providing that "Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except: a) with the consent of the individual whose personal information is collected;...[or] b) when necessary to provide a service or product requested by the individual..."

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.

This principle sets forth two fundamental premises regarding retention of information: (1) personal data should be kept and used in a lawful manner not incompatible with the purpose for which they were collected, which is recognized in Mexican doctrine and regulations as the principle of purpose, and (2) personal data should not be kept for longer than necessary for that purpose and in accordance with relevant domestic law.

Limited Use

Regarding the first premise, personal data and personal information must be handled for definite and lawful purposes, of which the person concerned has been advised and to which he or she has consented. Retention and use of personal information must be consistent with individuals' reasonable expectations, their relationship with the record keeper collecting the information, the notice(s) provided by the record keeper, and commonly accepted practices.

Personal data must not be kept or used for purposes other than those for which it was collected, except with the consent of the data subject or by the authority of law. The concept of "incompatibility" provides a certain measure of flexibility in this regard, allowing reference to the overall objective or purpose for which the individual's consent to collection was initially given. In this regard, the appropriate measure

may often be one of respecting the context in which the individual had provided his or her personal information.

For example, where an individual purchaser provides her name and mailing address to an online retailer, and that retailer in turn discloses the consumer's name and home address to the shipper so that the purchased goods may be delivered to the purchaser, this disclosure is clearly a "compatible" use of personal data. However, if the online retailer disclosed the consumer's name and home address to another type of retailer or marketer for purposes unnecessary for and unrelated to the completion of the consumer's online transaction, it would most likely be an "incompatible" use of the consumer's data and not allowed unless the consumer offers his or her express consent.

Limited Retention

Moreover, personal data may be kept only as long as required by the purpose for which it was collected and as prescribed by relevant domestic law. A limitation on data retention is required by modern technological realities. Because the cost of data storage has been reduced so sharply, it may often be less expensive for many record keepers to store data indefinitely rather than to review and delete unnecessary data. Yet unnecessary and excessive retention of personal data clearly has privacy implications. As a general rule, therefore, data must be disposed of when it is no longer needed for its original purpose or as otherwise required by national law.

However, it is not intended to suggest that record keepers must *always* delete data when no longer needed. Individuals may choose to consent, either expressly or by implication, to the use and retention of their personal information for additional purposes. Relevant domestic law imposes explicit legal requirements for data retention.

Moreover, a record keeper may have legitimate legal reasons to retain data for a certain period of time even if not explicitly required. For example, employers may retain records on former employees, or doctors may retain records on their former patients, in order to protect themselves against certain types of legal actions, such as medical malpractice, wrongful discharge, etc. Record keepers may retain personal information for periods longer than reasonably necessary:

- to provide services to individuals, in order to comply with other legal obligations,
- to protect the rights, safety or property of the individual, the record keeper, or a third party, or
- if the personal information is de-identified or aggregated so that it can no longer reasonably identify individuals, computers, or other devices.