Creation of a Global Privacy Standard

By Commissioner Ann Cavoukian, Ph.D.

Introduction

In 2005, at the 27th International Data Protection Commissioners Conference in Montreux, Switzerland, I chaired a Working Group of Commissioners. This Working Group was convened for the sole purpose of creating a single Global Privacy Standard. Faced with globalization and convergence of business practices, regardless of borders, I thought there was a pressing need to harmonize various sets of fair information practices into one Global Privacy Standard. Once such a foundational policy piece was in place, then businesses and technology companies could turn to a single instrument for evaluating whether their practices or systems were actually privacy enhancing, in nature and substance.

While attempting to develop a single law on data protection was beyond our reach, I was confident that we could develop a single privacy instrument, globally. In advancing my objective to develop a harmonized set of fair information practices, my office embarked on the preliminary work of conducting a "Gap Analysis." This was the process of comparing leading privacy practices and codes from around the world, comparing their various attributes, and the scope of the privacy principles enumerated therein. We identified the strengths and weaknesses of the major codes in existence and then tabled our Gap Analysis with the Working Group of Commissioners.

In the months that ensued, we embarked upon the work of harmonizing the principles into a single set of fair information practices. This led to the development of the attached Global Privacy Standard (GPS), which builds upon the strengths of existing codes containing time-honoured privacy principles and, for the first time, reflects a noteworthy enhancement by explicitly recognizing the concept of "data minimization" under the "collection limitation" principle.

After successive drafts of the GPS were developed, revised and circulated for review, the attached final version of the GPS was formally tabled and accepted in the United Kingdom, on November 3, 2006, at the 28th International Data Protection Commissioners Conference.

Objective

The objective of the Global Privacy Standard is to form a set of universal privacy principles, harmonizing those found in various sets of fair information practices presently in existence.

The Global Privacy Standard draws upon the collective knowledge and practical wisdom of the international data protection community.

Scope

The Global Privacy Standard reinforces the mandate of privacy and data protection authorities by:

- focusing attention on fundamental and universal privacy concepts;
- widening current privacy awareness and understanding;
- stimulating public discussion of the effects of new information and communication technologies, systems, standards, social norms, and laws, on privacy; and
- encouraging ways to mitigate threats to privacy.

The GPS informs developers and users of new technologies and systems that manage or process information. The GPS may be particularly useful when developing information and communication technology standards, specifications, protocols, and associated conformity assessment practices.

The GPS can assist public policymakers when considering laws, regulations, programs and the use of technologies that may impact privacy. The GPS can equally assist businesses and developers of technology that may have an impact on privacy and personal information.

The GPS addresses privacy concerns for decision-makers in any organization that has an impact on the way in which personal information is collected, used, retained, and disclosed.

The GPS is not intended to pre-empt or contradict any other laws or legal requirements bearing upon privacy and personal information in various jurisdictions.

GPS Privacy Principles

1. Consent: The individual's free and specific consent is required for the collection, use or disclosure of personal information, except where otherwise permitted by law. The greater the sensitivity of the data, the clearer and more specific the quality of the consent required. Consent may be withdrawn at a later date.

2. Accountability: Collection of personal information entails a duty of care for its protection. Responsibility for all privacy related policies and procedures shall be documented and communicated as appropriate, and assigned to a specified individual within the organization. When transferring personal information to third parties, organizations shall seek equivalent privacy protection through contractual or other means.

3. Purposes: An organization shall specify the purposes for which personal information is collected, used, retained and disclosed, and communicate these purposes to the individual at or before the time the information is collected. Specified purposes should be clear, limited and relevant to the circumstances.

4. Collection Limitation: The collection of personal information must be fair, lawful and limited to that which is necessary for the specified purposes.

> **Data Minimization --** The collection of personal information should be kept to a strict minimum. The design of programs, information technologies, and systems should begin with non-identifiable interactions and transactions as the default. Wherever possible, identifiability, observability, and linkability of personal information should be minimized.

5. Use, Retention, and Disclosure Limitation: Organizations shall limit the use, retention, and disclosure of personal information to the relevant purposes identified to the individual, except where otherwise required by law. Personal information shall be retained only as long as necessary to fulfill the stated purposes, and then securely destroyed.

6. Accuracy: Organizations shall ensure that personal information is as accurate, complete, and up-to-date as is necessary to fulfill the specified purposes.

7. Security: Organizations must assume responsibility for the security of personal information throughout its lifecycle consistent with the international standards that have been developed by recognized standards development organizations. Personal information shall be protected by reasonable safeguards, appropriate to the sensitivity of the information (including physical, technical and administrative means).

8. Openness: Openness and transparency are key to accountability. Information about the policies and practices relating to the management of personal information shall be made readily available to individuals.

9. Access: Individuals shall be provided access to their personal information and informed of its uses and disclosures. Individuals shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Compliance: Organizations must establish complaint and redress mechanisms, and communicate information about them to the public, including how to access the next level of appeal. Organizations shall take the necessary steps to monitor, evaluate, and verify compliance with their privacy policies and procedures.

Published: November 8, 2006