

A structure for PRIVACY

Considerations and best practices for implementing a privacy policy in your organization. *by Adriaan Veldhuisen*

In *Privacy and Freedom* (1967), Alan Westin formulated the classic early definition of privacy: “Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others.”

This definition evolved into The Privacy Act of 1974 (U.S.) in response to concerns about how the creation and use of computerized government databases might affect individuals’ privacy rights. From that point, privacy has become a set of “privacy principles and practices,” often containing some or all of the following composite requirements:

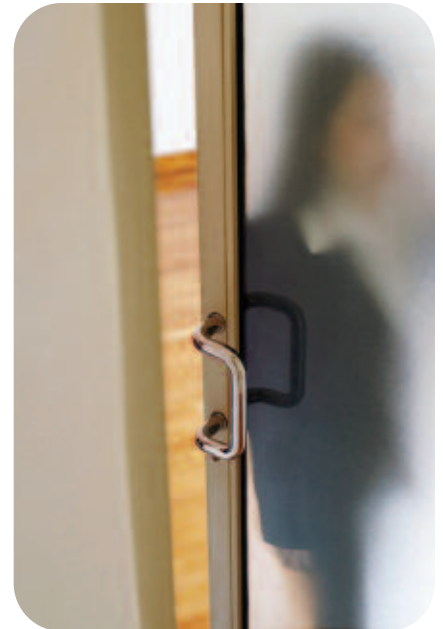
- > Notice and awareness
- > Choice and consent
- > Access by the subject of the personal information
- > Information quality and integrity
- > Update and correction
- > Enforcement and recourse

Influence of law on privacy

The recently completed “Analysis of Privacy Principles: An Operational Study” published by the International Security, Trust and

Privacy Alliance (ISTPA) reviews most of the privacy regulations worldwide. Based on this review, ISTPA derived a set of operationally focused working definitions, taking a practical approach to huge variations in language and the differing placement of many principles/practices in each regulation.

There is value in developing what the ISTPA calls “composite operational definitions” for fair information practice (FIP) principles. The composites incorporate primary operational characteristics of each FIP and can be useful in a number of ways. Foremost, they can provide you with a basis for mapping privacy requirements. The composites do so by establishing categories of requirements for your business processes and systems into which more granular requirements can be placed. Such composites can also be used to clearly link requirements that may fall into more than one category. For example, data quality



includes data destruction, which also implicates security and safeguards.

ISTPA Privacy Framework

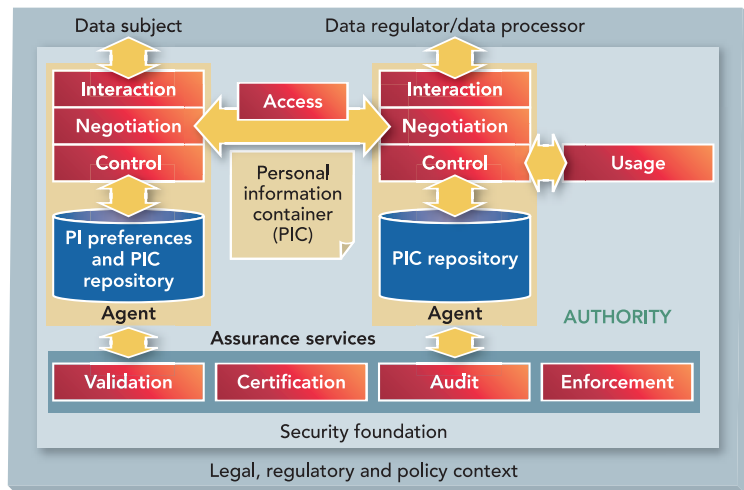
Without a common framework for analyzing the privacy issues and options, the policy debate over specific and emotionally charged privacy issues is difficult. The ISTPA Privacy Framework was developed to be a clearly defined and standardized set of operational privacy controls.

The figure on page 32 shows an example set of the privacy framework services and

Teradata is a founding member of the International Security, Trust and Privacy Alliance (ISTPA). The ISTPA is a non-profit alliance of companies and organizations that designed a Privacy Framework as a proactive tool that is able to support businesses in developing and managing their own privacy policies. For more information on the ISTPA and its recent study, visit www.istpa.org. And, for definitions of each of the 11 restructured requirements ISTPA accepted, visit TeradataMagazine.com for an expanded version of this article.



Figure ISTPA Privacy Framework



Through a logical configuration of the services in the ISTPA Privacy Framework with an agent service representing both the subject and the data requestor, security services are available to all the privacy services.

how they support data subject and data requestor interactions. In this example, the agent service represents a data subject and data requestor; each representative agent draws upon a set of assurance services (validation, certification, audit and enforcement) to protect agent interactions.

These assurance services provide additional functionality in managing personal information exchanges and processing. Each service works with the other services as needed in support of privacy requirements, independent of underlying platform and technology, giving implementers a reusable set of services to better manage and address privacy legal requirements that are complex and often difficult to interpret.

As an operational set of privacy services, this framework represents a comprehensive translation of legal and regulatory requirements into a set of interoperable services that assists architects, business process engineers and compliance professionals as a foundation to address and manage privacy as it evolves. The FIPs can be overlaid onto this example demonstrating how the legal principles are supported by the privacy services.

Almost every industry uses a data warehouse for sensitive information from consumers or personnel, and it always falls under regulatory governance. Although FIP principles are often viewed as simple concepts, implementing the FIP is not simple at all. The FIP principles have huge variation within and across regulations. To enable more systematic automation of privacy policies, at a minimum, the major requirements of each FIP should be abstracted for use in examining your policies and implementing practices. **T**

Adriaan Veldhuisen is a board member of ISTPA and holds three patents on privacy. He is a Teradata Certified Master and member of Teradata R&D, Product Management Team. He is responsible for setting the development requirements for Privacy and Security in Teradata releases.

Privacy implementation and best practices

Drivers for implementing privacy controls are compliance, data protection and meeting business objectives. Implementation of controls requires forethought and careful consideration. However, it also requires flexibility to adapt plans and best practices into a customized approach for the data warehouse to be continuously improved for ongoing success. Basic elements of consideration include:

I. Discover the privacy requirements:

- 1) Choose and adapt regulatory privacy principles that most apply to your business.
- 2) Develop and agree on a comprehensive privacy strategy for your business or division.
- 3) Develop a privacy program with clear responsibilities and obtain buy-in from your executives.

II. Develop a privacy program:

- 1) Translate your privacy program into published and actionable procedures for stakeholders.
- 2) Develop an information classification scheme that will be governed by the privacy program.
- 3) Particularly include the online environment in your information classification.
- 4) Develop user and operator classification of sensitive information (roles) including partners.

III. Deploy privacy implementation:

- 1) Protect your sensitive information with physical, technical and procedural safeguards.
- 2) Plan actions and communication before privacy incidents happen, ready to execute.

IV. Audit and maintain for compliance:

- 1) Audit internally and prepare for any external audits to which you will be subjected.
- 2) Institute control feedback and continuous improvement of your privacy implementation.