The ISTPA Privacy Framework

International Security, Trust, and Privacy Alliance

ISTPA Framework Project

Acknowledgments: **The ISTPA Framework Project members have worked tirelessly to identify and define the privacy services, mechanisms and use cases described below. Many of the ISTPA members have provided insight and commentary, but special thanks are due for**

Lark Allen
Kevin O'Neil
Drummond Reed
Gary Roboff
Geoffrey Strongin
Betty Whitaker
Michael Willett

George Jelen was especially devoted to the work of the Project, contributing content and insightful commentary. He kept us focused. In memoriam, we dedicate this work to George.

Introduction:

Privacy concerns have emerged as the #1 inhibitor to rapid adoption of the Web as a marketing channel to the consumer. What personal information is being requested from me and where is it being distributed? Do I have any control over such distribution? What recourse do I have in the event that my personal information is improperly handled?

Privacy has become a very public and personal issue. On the one hand, businesses want to know more about you and your buying habits, in order to deliver specific products and services that are of interest to you. On the other hand, most people feel that personal information is "personal" and should be shared only at the discretion of the subject. The speed and ubiquity of the Web have collapsed the logical "distance" between people and businesses and brought increasing pressures on managing the flow of personal information.

Privacy is a global issue. In the U.S., privacy legislation and regulation are emerging in specialized sectors, such as health and financial records, while industry generally is supporting self-regulation. In Europe, the European Union has established broad regulations over the collection, use, and dissemination of personal information for its member countries and those countries to which personal information is transported. Harmonizing the U.S. and European approaches to privacy has led to delicate and protracted negotiations, culminating in the *safe harbor agreement*, which strikes a balance between the broad legislative and the more sector-based and self-regulatory approaches.

Privacy focuses on how personal information is collected, used, and distributed. The high-level principles that govern the proper handling of personal information include notice and awareness of what personal information is being requested or collected, choice and consent over that collection, individual access and correction capability for personal information already collected, and recourse in case the information is improperly collected, used, or distributed. These principles do not inherently suggest how to implement the appropriate tools and lower-level functionality needed to "solve" the privacy problem.

The Privacy Framework is an analytic tool that satisfies the various privacy principles and fair information practices, but encourages the description of privacy implementations.

The purpose of this paper is to describe the Privacy Framework being developed by the Framework Project of the International Security, Trust, and Privacy Alliance (ISTPA).

Definitions:

Over a century ago, Supreme Court Justice Louis Brandeis defined privacy as "the right to be let alone", which he said was one of the rights most cherished by Americans.

More recently, Alan Westin (1967) has defined privacy as the right to control information about oneself, even after divulging it to others; the right of individuals to determine for themselves, how, when and to what extent information about them is communicated to others.

Webster's dictionary lists privacy as the quality or state of being hidden from the observation or activities of other persons, freedom from undesirable intrusions; and security as the freedom from danger or anxiety.

The following concise definitions have been developed by the Framework Project and are consistent with the related business challenges:

privacy: proper handling of personal information, consistent with the preferences of the subject.

security: establishment and maintenance of measures to protect personal information.

personal: refers to information related to an individual or to entities other than individuals. For example, corporate entities may have a concern about 'personal' information related to the corporation.

trust: a consumer *feeling* that depends on delivering value, while providing sustainable security and proper and agreed-to handling of personal information throughout its life cycle.

ISTPA:

The International Security, Trust, and Privacy Alliance (www.istpa.org) is a global alliance of companies and technology providers working together to provide objective and unbiased research and evaluation of privacy standards, tools, and technologies, and a privacy framework for building process-oriented and technology solutions.

ISTPA Key Goals:

- **Researching and developing an objective privacy framework for the protection of personal information about consumers; and protection of organizational data in jurisdictions where the law requires or allows it;**
- **Creating proof of concept demonstrations of new privacy standards, tools, and technologies;**
- **Defining the relationship between security, privacy, integrity, and trust;**
- **Devising strategies that ensure compliance with regulatory and legal privacy requirements worldwide;**
- **Providing objective guidance on privacy standards, tools, and technologies to the member companies;**
- **Sponsoring forums for the discussion of privacy issues and technology solutions;**

- **Serving as the voice and resource for industry on privacy issues and technology solutions.**

ISTPA Working Groups

ISTPA has two primary working groups: Framework and Proof of Concept.

Framework is responsible for developing and promoting an objective, analytic framework for achieving security, privacy, integrity, and trust in all forms of communications worldwide.

Proof of Concept is responsible for designing, organizing, and managing objective consumer research and implementation, together with demonstration projects to test the market value, management and usability of technologies supporting security, privacy, integrity, and trust, and objectively evaluating the facts developed.

ISTPA can help your company understand and address privacy needs and work with other industry leaders to build or implement technology solutions.

Privacy: The Business Imperative

Privacy is now where security was years ago. For many years, security issues and challenges have benefited from the existence of a technology framework and a recognized, even standardized, set of security technologies, including cryptography, hash functions, public-key infrastructure, and secure communication protocols. Lately, the OpenGroup has modified the traditional OSI-based security infrastructure to accommodate a richer set of business requirements; broadening security from a protectionist focus to being an enabler of the mandates of electronic business [APKI].

Similar pressures now exist to provide an enabling, technical infrastructure for the provision of *privacy* in a business context.

Multiple forces are interacting to magnify the concerns for privacy in modern society. The speed, ease of use, and ubiquity of the Internet have made the gathering, use, and distribution of personal information almost instantaneous. Couple that technical ability with the consumer demand and the business competitive pressures to "know the customer"; to customize and target merchandising to the specific preferences and interests of the consumer. The result is an increasing potential to misuse and abuse personal information.

Information, even personal information, is essential to the proper functioning of modern society. The desire is not to banish personal information, but to develop strict and enforceable means to ensure the *proper* handling of personal information. Improper handling of personal information will expose a business to potential legal and fiduciary consequences, as well as jeopardize brand identity. The bottom line is to sustain consumer trust.

Privacy Principles and Practices

Whereas security solutions can draw on a rich store of technologies and products, the privacy landscape is much less mature. Instead, privacy "solutions" consist of privacy principles and 'fair information practices' that are subject to a range of interpretations and manual applications. More importantly, the principles and practices do not inherently suggest specific supporting technologies as part of the privacy solution.

A widely-recognized set of privacy principles include:

- **disclosure: informing the subject when personal information is collected.**
- **relevance: collecting only personal information pertinent to the application.**

- **participation: allowing subject choice over collection and distribution.**
- **collection limitations: limiting the types of information collected.**
- **use limitations: limiting the subsequent use of collected information.**
- **accountability: ability to address the improper handling of personal information.**
- **security: protecting personal information.**
- **verification: checking the validity of personal information.**

The privacy principles are self-explanatory, but "standalone" in the sense that interrelationships among the principles are not intuitive. How are Disclosure and Relevance related? How is Security implicated into the other principles? Most importantly, how is the subject/consumer positioned? And, what is the overall 'control' mechanism that ensures adherence to privacy preferences?

At a lower logical level, the following privacy *practices* could be used to implement the privacy principles, but the interrelationship among the practices is left to the imagination:

Notice and Awareness
Choice and Consent
Individual Access
Information Quality and Integrity
Update and Correction
Enforcement and Recourse

The operational ingredients, such as the consumer, requestor of information, interfaces, control methods, and the cohesion needed to provide an analytic framework are still missing. However, a better imagery of the 'life cycle' of personal information is available through the privacy practices. Notice and awareness inform the consumer and data subject of the privacy information collection, use, and distribution desires of a requestor. Choice and consent allow the data subject to agree or disagree to the requestor requests. Individual access allows the data subject to view previously collected personal information. Information quality and integrity provide the necessary security and protections. Update and correction are applied, as needed. Finally, enforcement and recourse are available to handle exception conditions.

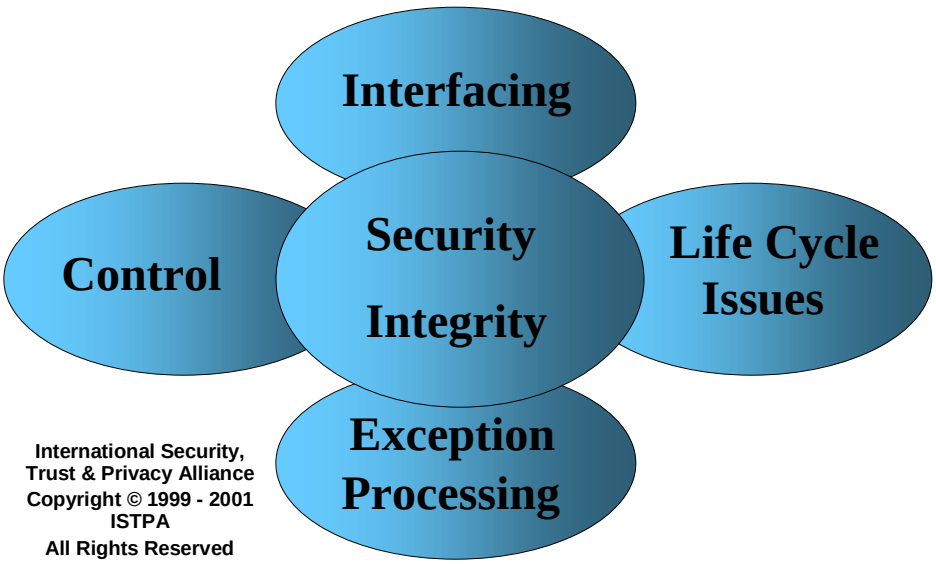
Still, a unified operational framework is needed in which the coordination and interaction of privacy services can be described.

"Operational" Framework

In order to evolve the privacy practices into an operational framework, we must think like a programmer. What ingredients are needed to facilitate the execution of functions and the interplay with the surrounding environment? Can the privacy practices be largely reduced to a computer program in which jurisdictional, legal, and administrative variability is handled through customized input parameters?

A top-down design would first recognize the need to 'interface' the external participants with the internal functions; supporting input of personal data and related parameters and the output of collection notices. A broad 'control' function masterminds the proper handling of personal data. 'Life cycle issues' must be traced, especially as personal data is transferred beyond the immediate control of the subject. As unacceptable or improper activities occur, 'exception processing' would be invoked. Overall, 'security and integrity' functions would guarantee that the people, credentials, and processes are sufficiently authenticated and authorized.

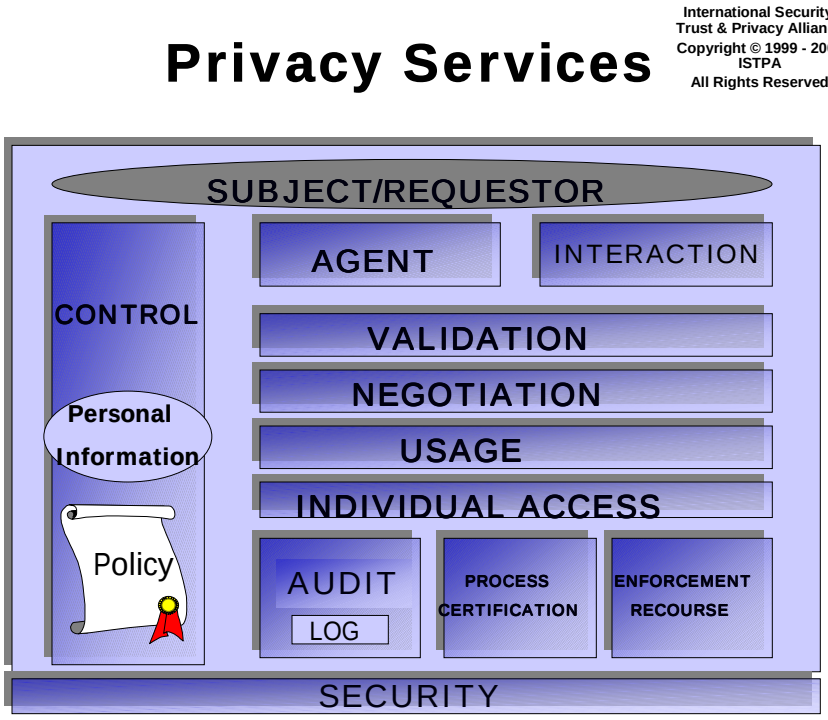
"Operational" Requirements



With these operational facilities in mind, the privacy practices can be structured into a process-oriented, analytic framework.

Privacy Framework

The ISTPA Framework Project team started with the privacy *p*rinciples and *p*ractices (and privacy *p*olicies, *p*rocedures, and even a few *p*rotocols; the privacy 5 "*p*"s) and applied analytic and reduction techniques to define a set of privacy *services* and supporting *mechanisms*. The interrelationship of these services and the interaction with the data subject, the agent, the requestor, the collector, and the authorities was also delineated. Since security is an essential element in the proper handling of personal information, the appropriate security services and mechanisms are seamlessly integrated into the Privacy Framework. The recent work of the OpenGroup standards organization (www.opengroup.org/security) was adopted. The OpenGroup has identified a set of security services and supporting mechanisms, together with the necessary interactions, functionality, and even specific protocols, where appropriate. The structural properties of the privacy and security services are consistent and complementary, contributing to a well-integrated Privacy Framework:



The analysis that led to the iterative refinement of the privacy services is suppressed here, but the current service list resulted from detailed and lengthy discussions of service functionality. The services needed to be "operationally" complete and encompassing of the privacy principles and practices. The following table gives a summary description of the privacy services:

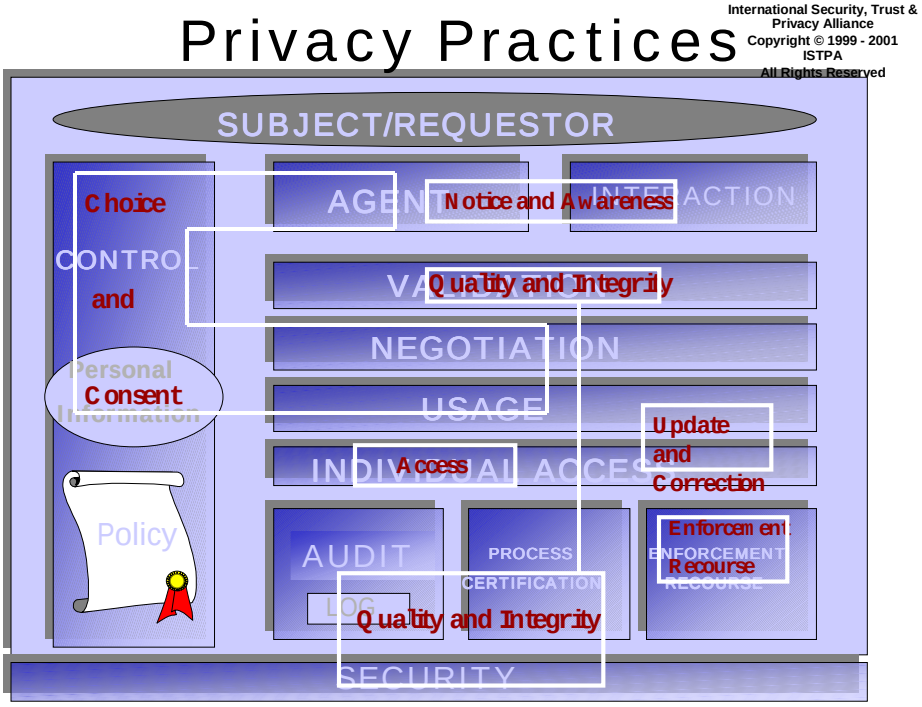
SERVICE	DESCRIPTION
Agent	**A software process acting on behalf of a data subject or a requestor to engage with one or more of the other Services defined in this Framework. Agent also refers to the human data subject in the case of a manual process.**
Interaction	**Handles presentation of proposed agreements from a data collection entity to a data subject; input of the subject's personal information, preferences, and actions; and confirmation of actions. To the extent the data subject is represented by an Agent, this service comprises the interface to the Agent.**
Control	**Handles the role of "repository gatekeeper" to ensure that access to personal information stored by a data collection entity complies with the terms and policies of an agreement and any applicable regulations.**
Validation	**Handles checking for correctness of personal information at any point in its life cycle.**
Negotiation	**Handles arbitration of a proposal between a data collection entity and a data subject. Successful negotiation results in an agreement. Negotiation can be handled by humans, by agents, or any combination.**
Usage	**Handles the role of "processing monitor" to ensure that active use of personal information outside of the Control Service complies with the terms and policies of an agreement and any applicable regulations. Such uses include derivation, aggregation, anonymization, linking, and inference of data.**
Individual Access	**Handles the data subject's ability to view, correct, and update personal information and agreements. (Note that modification of non-modifiable agreements requires renegotiation of the agreement.)**
Audit	**Handles the recording and maintenance of events in any Service to capture the data necessary to ensure compliance with the terms and policies of an agreement and any applicable regulations.**
Process Certification	**Handles validation of the credentials of any party involved in processing of a personal information transaction.**
Enforcement/ Recourse	**Handles redress when a data collection entity is not in conformance with the terms and policies of an agreement and any applicable regulations.**

The Agent and Interaction Services handle the exchange with 'external' entities and represent the data subject in activities involving other Services. The Control Service enforces the corporate/individual privacy policy. The Negotiation Service is invoked by the Agents of both the data

subject and the personal information requestor to arbitrate an agreement for the collection of specified information. The agreement is then bound (possibly, cryptographically) to the personal data throughout its life cycle. The Usage Service handles the enforcement of agreements when personal information is manipulated into other forms, such as aggregation. The Individual Access Service allows the data subject to control the integrity of personal information, while the Process Certification Service validates credentials. The Audit Service maintains the log for recording any designated exception conditions that could later be used by the Enforcement/Recourse Service to provide remedy for the improper handling of personal information.

The life cycle of personal information involves time when the subject does not have immediate or physical control over the information. Yet, the subject wants to maintain vicarious control over subsequent transfer and usage. The transfer/usage agreed to by the subject should be robustly attached to and travel with the personal information, so that subsequent actions will be based on the consumer preferences.

The original fair information practices map to the Privacy Framework as follows:



The interested reader will appreciate that large portions of the Privacy Services could be "programmed" for computer and automatic (and transparent) implementation and that the various entities being manipulated (eg, personal information, policy) could be represented in object technology. Recall that the original ambition of the Framework Project was to provide an analytic and technology-oriented context for satisfying the privacy principles/practices, so that solution mechanisms could be defined. Security, privacy's sister science, has enjoyed such technology solutions for some time.

The Framework Project has drafted a detailed description of the mechanisms and interactions that compose the Privacy Framework. That draft will soon be available on the ISTPA Web site (www.istpa.org). The reader is invited to submit suggestions and corrections to mwillett@fiderus.com.

Privacy Mechanisms

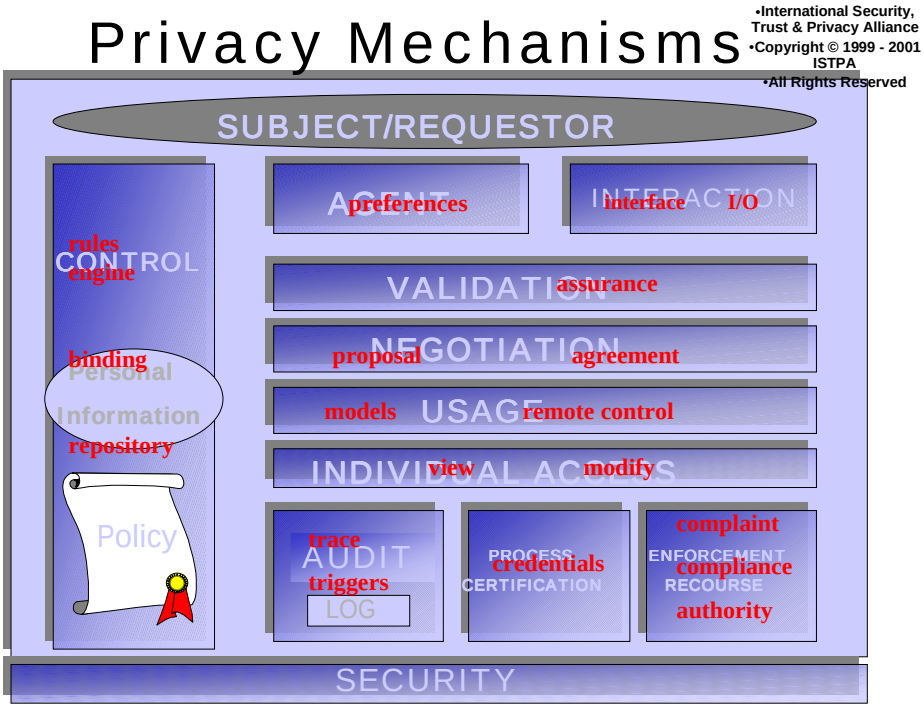
Each privacy Service is composed of *mechanisms* that collectively implement that Service and that provide guidelines as to what specific technologies (even products) could be used to achieve each mechanism.

For example, the Control Service includes a rules engine and a binding mechanism for robustly pairing personal data with agreements.

The Negotiation Service must:

- **create and transfer a proposed agreement**
- **receive a counterproposal or conditional agreement**
- **arbitrate the agreement between the data subject and requestor**
- **transfer the agreement to the Agent and Control Services**

The mechanisms of the Individual Access Service provide a means for data subjects to view and modify the personal information associated with the subject by a data collection entity. Specifically, the Individual Access Service must provide a means to locate the access mechanism provided by the data collection entity; a means of authenticating the data subject; a means of viewing the personal information, including the permissions granted under a data collection agreement; a means of modifying or deleting the personal information, permissions, or the agreement itself; and a means of confirming such changes have been accepted and recorded by the data collection entity. Optionally, the Individual Access Service can provide access to the Enforcement and Recourse Service, if the data subject believes the terms of a data collection agreement have been violated.



The mechanisms for each privacy Service are documented in the ISTPA Privacy Framework document (to appear).

Use Cases

The test of robustness and completeness of the Privacy Framework is to determine if a broad range of real-world scenarios related to privacy can be realized as interactions among the Privacy Services. We invite the public to participate in this use-case exercise.

Consider the following use case; first, strictly from the point of view of the consumer. Personal information and preferences (i.e., constraints on the use of that personal data) are configured. While searching for a bargain on the Web, the consumer engages with a commercial site, which offers the consumer a 10% discount on a widget in exchange for selected personal information (i.e., age, family income). Since the deal matches the consumer preferences, the agreement is struck and the exchange occurs transparently. The Consumer is not bothered with the detail, but the 10% discount is applied to the purchase. Later, the personal information is aggregated with other consumer data, in violation of the previous

agreement. The violation is reported to an external watchdog agency, which takes appropriate action against the commercial site owner.

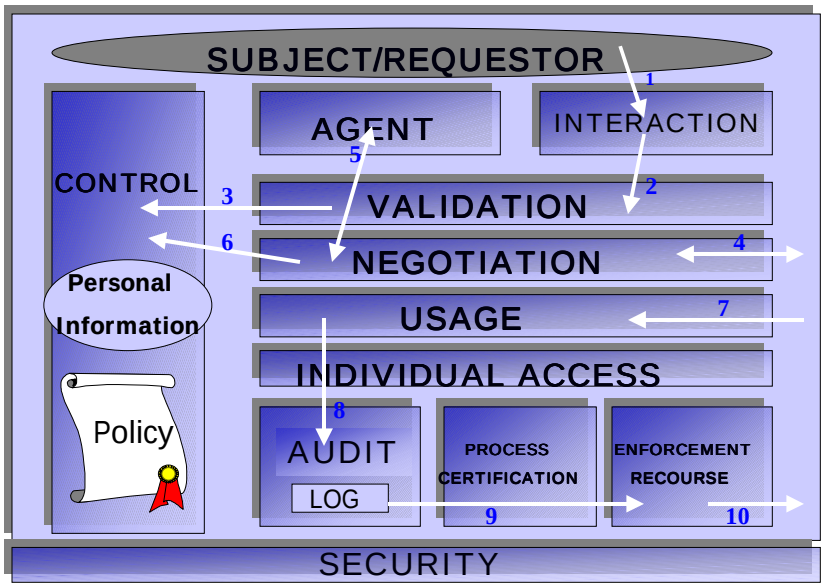
Now, let's examine what is going on "under the covers" (see the numbered chart below):

1) **personal information and preferences are received by the Interaction Service,**
2) **passed to the Validation Service, then**
3) **stored securely by the Control Service.**
4) **The commercial site initiates activity with the Negotiation Service, with**
5) **the Agent Service handling the arbitration for the consumer.**
6) **The agreement is stored by the Control Service and bound to the personal data before being transferred to the commercial site.**
7) **The Usage Service learns that the commercial site aggregates the personal information with other data, in violation of the agreement.**
8) **The violation is recorded in the Audit Service log, which has a trigger set for just such an occurrence.**
9) **The violation is reported to the Enforcement/Recourse Service,**
10) **which is configured to report such incidents to the outside watchdog agency.**

Once configured, the sequence of actions involving the various Services will happen transparently, without surfacing to the consumer. Of course, any security safeguards, like personal information confidentiality or commercial site authentication, would be provided by the Security Services.

The interested reader is encouraged to think of other use-case scenarios that flex the full functionality of the Privacy Framework.

Use Case Scenario



Summary

The ISTPA/Framework Project is charged with developing an administrative, technical, and legal Privacy Framework within which to provide functionality that satisfies the privacy principles and practices. A layered analysis was adopted, by which the principles/practices were morphed into privacy *services*, which in turn are realized by underlying privacy mechanisms. These services call on and integrate with the security services defined by the OpenGroup, to satisfy the security principle. The Privacy Framework is tested for robustness by considering a variety of use case scenarios.

Critiques/corrections should be sent to Michael Willett, chair of the ISTPA/Framework Project, at mwillett@fiderus.com.