A technical discussion of privacy protection
July 2002

Tivoli software

Enable your applications for privacy with IBM Tivoli Privacy Manager for e-business

Contents

Introduction

A growing number of privacy regulations and consumer demands for privacy protection have significantly impacted companies around the world in recent years. Advances in information technology—both online and offline—have led to heightened concerns about the way companies use and protect the personally identifiable information (PII) they collect. Under many current laws and regulations, companies or organizations that collect PII are considered the custodians of that information, and as such, they are responsible for obtaining the data owner's consent before using the information. Increasingly, businesses have responded to data privacy concerns by working to incorporate privacy practices into their business processes. They have appointed chief privacy officers (CPOs), crafted comprehensive privacy policies and formed privacy management teams all in attempts to meet today's expectations.

The stakes are especially high for companies competing in specific industries, such as healthcare and financial services, that must comply with an extensive set of rules about data privacy. Otherwise, they can be subject to large fines, and in some cases, imprisonment. Worse, the damage to the company's reputation can be several times the cost of the fine in terms of lost opportunity and diminished brand appeal. Similarly, government agencies may find it difficult or impossible to convince people to use online services if the agencies cannot demonstrate that private data is adequately protected against misuse.

The costs associated with privacy compliance can be daunting for companies or for government agencies—easily totaling millions of dollars annually for large organizations that use manual processes to create, implement and enforce their data privacy policies.

New software product from IBM

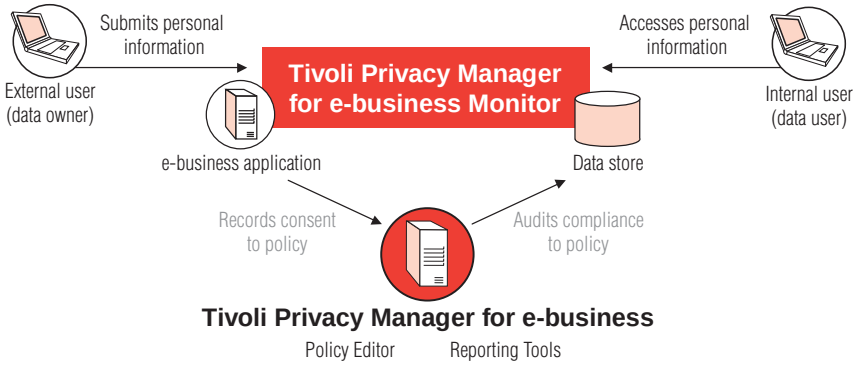
IBM has introduced a new software product—IBM® Tivoli® Privacy Manager for e-business, Version 1.1—that is designed to help large organizations build privacy policies and practices directly into their e-business applications and infrastructure. Tivoli Privacy Manager for e-business can be used to reduce costs by helping automate many privacy compliance activities. It can also help improve the overall management of privacy policies and processes by providing an infrastructure to support the consistent enforcement of those policies across the organization.

Highlights

Tivoli Privacy Manager for e-business can help automate many privacy compliance activities and provide an infrastructure to support consistent enforcement of privacy policies.

Organizations can use Tivoli Privacy Manager for e-business to perform five primary tasks:

- *Define the privacy policy and convert it from prose to Platform for Privacy Preferences (P3P) format*
- *Deploy the privacy policy across applications and resources*
- *Record end users' consent to the privacy policy*
- *Monitor and enforce access to private data, in keeping with the policy*
- *Create audit trail reports*



Components and functions of Tivoli Privacy Manager for e-business

Tivoli Privacy Manager for e-business is a Java™ 2 Enterprise Edition (J2EE™) application running on IBM WebSphere® that leverages the security infrastructure provided by IBM Tivoli Access Manager for e-business. Tivoli Privacy Manager for e-business provides the following components and functions:

- ***Policy Editor:*** *An advanced P3P interface that creates machine-readable privacy policies from written privacy policies. The Policy Editor helps privacy officers, legal counsel and IT staff work together to build privacy rules that integrate policy into practices.*

- ***Policy Deployment:*** *Links privacy policies to personal information by creating data types and then connecting data types to users, groups, storage locations and application requests. Tivoli Privacy Manager for e-business creates an infrastructure for "outsourcing" the maintenance of individual privacy preferences to end users—making it simple for them to opt in or opt out of the company's policies governing the use of personal information. The software automatically records the user's consent, helping organizations comply with privacy regulations and provide an auditable record of privacy practices.*
- ***Report Generator:*** *Generates enterprisewide reports, showing policies deployed, enforcement locations and audit trails detailing personal information management according to privacy policies. The Report Generator can also be used to generate individual reports showing how one person's data has been used by the enterprise. Audit reports can be stored in a DB2® database. They can be accessed online to provide immediate access to the usage history for personal information—whether to comply with internal audits and regulatory reviews or to respond to a data owner's request.*
- ***Administration Console:*** *The IT staff can manage and adjust the operating parameters of Tivoli Privacy Manager for e-business on an enterprise basis from one central console. The administration console provides comprehensive control over policies, storage locations, audit logs, preferences and consent. IT staff can use the administration console to update and journal privacy policies, enable and disable monitors and archive audit logs.*
- ***Tivoli Privacy Manager for e-business Monitor Software Deployment Kit (SDK):*** *The SDK contains a Java library that makes it simple to develop Tivoli Privacy Manager for e-business monitors for applications, middleware data repositories and other systems that persistently store privacy-sensitive information. This is a free development kit that can be used to extend the functionality of Tivoli Privacy Manager for e-business.*
- ***LDAP Monitor:*** *A "reverse LDAP proxy" that can monitor LDAP V3 message flows between an LDAP client application and an LDAP server, as well as enforce the privacy policy on clients attempting to access privacy-sensitive resources on the LDAP directory. This software code is offered as a reference implementation of the monitor SDK, to demonstrate how monitors are developed and deployed.*

Highlights

Tivoli Privacy Manager for e-business captures individual consent to enterprise privacy policies and then centrally monitors and enforces access based on that consent.

How it works

Traditional security (or access control) technologies do not go far enough to offer a comprehensive solution for privacy management. Access control technologies only focus on identifying users, determining what resources they will be allowed to use and deciding what simple actions (read, write, update or delete) they will be allowed to perform.

Tivoli Privacy Manager for e-business enhances traditional access control and single sign-on systems by incorporating two additional variables into access requests—the preferences of the "data owner" and a specific business purpose for which the data will be used.

Through the use of Submission and Access monitors associated with specific applications, Tivoli Privacy Manager for e-business is able to capture each individual's consent to enterprise privacy policies, and then monitor and enforce access based on that consent. A central server is used for defining the policies and generating audit reports. Deploying Tivoli Privacy Manager for e-business in an enterprise establishes a privacy management layer across applications and the IT infrastructure that helps the organization centrally manage private data and privacy policies.

Define policies

Using the Policy Editor, the CPO—or someone authorized to act in the CPO's role—begins by defining the company's privacy policies. A statement covering a healthcare provider, for example, might read as follows:

"Authorized doctors may access a patient's records for cancer medications for the purpose of treatment, but consent must be obtained before authorized researchers can access those records for the purpose of marketing experimental medications."

Highlights

The CPO takes this "human readable" policy and uses the Policy Editor facility to begin breaking down the policy into distinct components, such as groups, business purposes and data types. A "human-readable" policy, such as the one cited on page 5, might look like this after applying the Policy Editor:

Groups	Business purpose	Types
Authorized doctors	Treatment	Cancer medication
Authorized cancer researchers	Marketing experimental medications	

In general, the organization's privacy policies should be defined by people who understand the business and legal environment the organization faces and can address conceptual requirements from the perspective of applicable laws and business strategy. When defining policies with the Policy Editor, there is no need to refer to specific IT infrastructure elements, such as applications, systems or technologies. The individual responsible for setting and describing privacy policy does not have to be an expert in complex computing systems or techniques of IT management.

Deploy policies

The next step is to deploy the privacy policy. This is also accomplished through the Deployment Facility, which is generally used by someone authorized to act in the role of the IT staff. Policy deployment is considered an IT staff responsibility due to IT staff members' expert knowledge of the organization's customer profiler/storage system.

Tivoli Privacy Manager for e-business helps identify the resources in the environment where private or sensitive data is stored. It then classifies the data based on definitions in the Policy Editor.

Tivoli Privacy Manager for e-business helps the IT staff perform the two key tasks required for effective policy deployment. First, Tivoli Privacy Manager for e-business helps identify the resources in the environment where private or sensitive data is stored. Next, it classifies (or "tags") the data with one or more PII types, which have been defined in the Policy Editor. The Deployment Facility also assists in mapping the groups and purposes defined in the Policy Editor against the actual groups or roles recorded in the organization's underlying access control infrastructure (for example, the users and groups get defined in Tivoli Access Manager for e-business).

Highlights

Tivoli Privacy Manager for e-business helps determine the privacy policy that the data owner has consented to as well as the privacy policy that governs future access to this data.

After privacy policies are created and deployed, Tivoli Privacy Manager for e-business also helps manage how the policies are enforced across the enterprise. This includes the ability to automate the process of obtaining the end user's consent.

Record data owner's consent
The primary function of the Tivoli Privacy Manager for e-business monitors is to observe the data going in and out of monitored systems. When a monitor determines that new or updated PII has been submitted to the monitored system, the monitor automatically starts a session with the Tivoli Privacy Manager for e-business server to record information about the submission.

The Tivoli Privacy Manager for e-business server then creates a record of the identity of the person whose data is being submitted (data owner), records the time and date of the submission and automatically tags the PII with a data type, in accordance with established policies. From this "consent record," Tivoli Privacy Manager for e-business can determine both the privacy policy that the data owner has consented to and the privacy policy that governs future access to this data.

Tivoli Privacy Manager for e-business provides considerable flexibility in recording and managing consent, according to the policies the organization has set. Consent to a privacy policy can be assumed after the policy has been communicated to data owners through postal mail or e-mail. Consent can also be implied when end users submit PII or register to create an account. Very often, the end user's opt-in and opt-out choices can be provided at the time of their data submissions. Tivoli Privacy Manager for e-business simplifies the process of collecting and managing this consent data, with little or no intervention from the IT staff required.

Monitor and enforce policy compliance
Using Tivoli Privacy Manager for e-business software also allows the organization to automate the process of monitoring and enforcing access to data, based on the end user's consent.

The Tivoli Privacy Manager for e-business monitors are used to deliver this capability, automatically detecting when PII data is accessed in the monitored

systems. They then collect information to create an audit trail of the access events. By using user and group information provided by Tivoli Access Manager for e-business, the monitors identify whose data is being accessed, who is accessing the data (by application, by user or both) and the time and date when the access occurred.

This information is sent to the Tivoli Privacy Manager for e-business server, which uses PII tagging information to determine what policies should be enforced on the data in question. The server uses the information collected by the monitor to perform a privacy policy conformance check.

This conformance check automatically determines the answer to two critical questions:

- *Does the policy allow this sensitive data to be accessed for a valid purpose by this user?*
- *Did the owner of the data consent to the governing policy or policies?*

Tivoli Privacy Manager for e-business supports either one of two modes for conformance checking: runtime mode or near-time mode. The chosen mode of conformance checking will determine what actions are taken following the check.

In the runtime conformance checking mode, data accesses are blocked by the Tivoli Privacy Manager for e-business monitor until the Tivoli Privacy Manager for e-business server determines that the request conforms to governing privacy policies. If the attempted access is nonconforming, the monitor will deny or modify the data access attempt, as appropriate. This mode of conformance checking provides a high level of protection against unauthorized use of PII, but it also has the most impact on the performance of the monitored system.

When the near-time conformance checking mode is chosen, data accesses are not blocked at the time of the request. The Tivoli Privacy Manager for e-business monitor collects information to create an audit trail and sends it on to the Tivoli Privacy Manager for e-business server. The server then performs

a privacy policy conformance check on the access attempt and logs any nonconforming accesses. These log files can later be used to improve enforcement of privacy policies, to identify nonconforming users and so on. In addition, the Tivoli Privacy Manager for e-business server can be instructed to send alerts to high-level systems management consoles, such as IBM Tivoli Enterprise Console®, helping integrate privacy management activities with the organization's overall strategy for systems management.

Create audit trail
Tivoli Privacy Manager for e-business can also be used to comply with the requirements of specific privacy regulations by helping the organization create audit trail reports. These reports are generated from the records collected by the Tivoli Privacy Manager for e-business server whenever Tivoli Privacy Manager for e-business monitors detect submissions and accesses of PII across the computing environment.

The Tivoli Privacy Manager for e-business user interface can create and run reports covering many different aspects of the privacy policy environment—not just the submission or access of PII data. The records in the Tivoli Privacy Manager for e-business server can be used to generate:

- *Reports showing an enterprisewide perspective on the collection of PII, along with the policies that govern this data*
- *Audit trail reports for specific monitored systems to show conformant and nonconformant accesses*
- *Reports showing access to the PII of a specific data owner or owners, including reports detailing who accessed an individual's PII and for what purposes*

Integration with existing systems

Tivoli Privacy Manager for e-business offers the additional benefit of providing integration with many existing e-business resources. It includes an SDK to develop monitors for specific e-business applications. The SDK is designed to help organizations accomplish their privacy management tasks with little or no disruption to existing storage protocols or applications.

Highlights

With Tivoli Privacy Manager for e-business, users and data owners need to be defined only once, because the same registry can be applied from Web-based applications to mainframe resources.

A true middleware product, Tivoli Privacy Manager for e-business makes it possible to create an easy-to-manage privacy "layer" for the computing environment. For example, with Tivoli Privacy Manager for e-business the organization's existing user registry can be re-used across many different resources. Users and data owners need to be defined only once, because the same registry can be applied across the environment, from Web-based applications to mainframe resources.

Through the use of the SDK, integration can happen in three different areas of the IT environment:

- *Application and storage systems*
- *Enterprise abstraction layer*
- *Business integration and workflow*

Monitors can be written and placed on specific applications and storage systems. If the organization maintains a data abstraction layer, such as an LDAP directory or a data warehouse, Tivoli Privacy Manager for e-business monitors can also be placed in this layer, making it possible to add privacy management to any application that uses the data abstraction layer. Finally, organizations that use workflow tools or infrastructure can also add privacy management to automated processes, protecting privacy throughout these transactions.

Summary and conclusion

Tivoli Privacy Manager for e-business can help organizations meet the challenges of privacy management while providing the opportunity to enhance relationships with customers, employees and other business associates.

Tivoli Privacy Manager for e-business simplifies the administration and enforcement of privacy policies by turning "human-readable" policies into "machine-readable" policies that can be monitored automatically across the computing environment.

This innovative solution delivers a number of potential business benefits. It may help reduce the cost of administering privacy practices by providing an automated way to obtain the consent of data owners, record accesses to

personal information and generate compliance reports. Along with potentially reducing administrative costs, these automated functions may also mitigate the risks associated with using personal data by checking that the organization is complying with its posted privacy policies. Tivoli Privacy Manager for e-business provides a way to use the organization's IT systems to help drive compliance with privacy regulations and privacy policies.

IBM software integrated solutions

Tivoli Privacy Manager for e-business supports a wealth of other offerings from IBM software. IBM software solutions can give you the power to achieve your priority business and IT goals.

- *DB2 software helps you leverage information with solutions for data enablement, data management and data distribution.*
- *Lotus® software helps your staff be productive with solutions for authoring, managing, communicating and sharing knowledge.*
- *Tivoli software helps you manage the technology that runs your e-business infrastructure.*
- *WebSphere software helps you extend your existing business-critical processes to the Web.*

To learn more

For more information about privacy management products and integrated e-business infrastructure solutions from IBM, contact your IBM sales representative or visit **tivoli.com**/security

Tivoli software from IBM

An integral part of the comprehensive IBM e-business infrastructure solution, Tivoli technology management software helps traditional enterprises, emerging e-businesses and Internet businesses worldwide maximize their existing and future technology investments. Backed by world-class IBM services, support and research, Tivoli software provides a seamlessly integrated and flexible e-business infrastructure management solution that uses robust security to connect employees, business partners and customers.

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

07-02

The Tivoli home page on the Internet can be found at **tivoli.com**

The IBM home page on the Internet can be found at **ibm.com**

G325-6830-00