From Privacy Promises to Privacy Management

A New Approach for Enforcing Privacy Throughout an Enterprise

Paul Ashley
IBM Software Group
Gold Coast, Australia
pashley@au1.ibm.com

Calvin Powers
IBM Software Group
Raleigh NC, USA
cspowers@us.ibm.com

Matthias Schunter
IBM Research
Zurich, Switzerland
mts@zurich.ibm.com

General Terms
Enterprise Privacy Management, Privacy Policy, E-P3P

ABSTRACT

Regulations and consumer backlash force many organizations to re-evaluate the way they manage private data. As a first step, they publish privacy promises as text or P3P. These promises are not backed up by privacy technology that enforces the promises throughout the enterprise. Privacy tools cover fractions of the problem while leaving the main challenge unanswered.

This article describes a new approach towards enterprise-wide enforcement of the privacy promises. Its core is a new framework for managing collected personal data in a sensitive, trustworthy way. The framework enables enterprises to publish clear privacy promises, to collect and manage user preferences and consent, and to enforce the privacy promises throughout the enterprise.

One of the foundations of this framework is the "sticky policy paradigm" that defines a customer centric model for managing policies, preferences, and consent.

1. INTRODUCTION

Privacy is the right of individuals to determine for themselves when, how and to what extent information about them is communicated to others. The OECD defined a set of privacy principles [10] more than 20 years ago that struck a balance between the need for the free flow of information and the fundamental human right to privacy.

Recent advances in computer and communication technology has seen the amount of data flowing grow exponentially, but the technology to enforce the privacy principles has not accommodated this growth. Hence, we are in a world now where violations of privacy are a common occurrence. In response to these privacy violations many countries have enacted legislation to protect privacy. The core of the legislation is often based on the OECD privacy principles. Enacting the legislation has varied. In the EU [22], Canada [4] and Australia [3] for example, regulations for the protection of PII[1] that crosses industry sectors has been created. The United States has taken a sectorial approach, enacting separate regulations for health care [18], finance [19] and protection of children's data [8]. In either case the goals are clear - to give better protection to PII data.

Individuals are also reacting to privacy violations. Many people are aware that giving their PII to organizations may result in the data being used in ways the person never intended. This is being reported as one real inhibitor in the growth of on-line business. For example, one research report from Forrester Research [16] suggests that on-line commerce was reduced by US$15 billion in 2001 due to individual privacy concerns.

Because of regulations and reactions from individuals, some organizations are re-examining their management of PII. These organizations would like to be able to demonstrate that they are managing this data in a sensitive, trustworthy way. This includes having a well defined privacy policy, allowing users to make choices regarding the use of their PII, and enforcing the policy and user preferences across the whole organization.

To address this growing need for privacy management, many companies are marketing privacy tools that are supposed to help address the privacy problem. These tools only address a small part of the problem, and organizations don't yet have the tools to allow them to fully manage and enforce privacy.

The missing piece is enterprise privacy management technology. This technology must be the focal point for defining and enforcing an enterprise wide privacy policy. It must enable monitoring, enforcement and auditing of the the policy across the whole IT infrastructure of the organization. It must also allow for management and enforcement of individual privacy preferences.

1.1 Overview

We describe the new concept of privacy management systems for enterprises. We define a comprehensive framework

New Security Paradigms Workshop '02, September 23-26, 2002, Virginia Beach, Virginia.
Copyright 2002 ACM ISBN 1-58113-598-X/02/0009 ...$5.00

[1] We use the term PII for any personally identifiable information that relates to an identifiable individual.

that is based on the "Sticky-policy Paradigm" that mandates that customer-consented policies stay associated with the collected data. Unlike any existing technology, our technology covers not only "consent" and "collection" but also enterprise-internal cataloging, control, and reporting.

Section 2 reviews the reasons for organizations to be concerned about the way they handle PII. Section 3 gives an overview of current privacy technology, gives a classification for each type of technology, and points out the missing pieces. Section 4 outlines our paradigm for enterprise privacy management from a functional point of view. Section 5 outlines our building blocks to fulfill the privacy requirements. We finish with our conclusions.

2. ORGANIZATIONS ARE CONCERNED ABOUT PRIVACY

Privacy is an important concern for any organization that deals with PII. There are a number of risks to an organization if it does not manage its PII correctly.

2.1 Legislative Penalty

Recently there has been new privacy legislation enacted in many parts of the world. Most of these laws incorporate rules governing collection, use, retention and distribution of PII. It is up to an organization to ensure that it is compliant with any legislative requirements or industry regulations that apply to it.

There are already many examples of organizations suffering penalties from regulators. In the United States recently Toysmart [5] felt the weight of the Federal Trade Commission for privacy violations. Toysmart faced the very first charge related to violation of the Children's Online Privacy Protection Act (COPPA) [8].

2.2 Brand and Reputation Erosion

Business relationships are built on trust. Trust means that when doing business with an organization it is expected that the organization will conduct itself with integrity and its behavior will be predictable and consistent. Trustworthy organizations are more likely to attract business.

Organizations that demonstrate good privacy practices can build trust. By promoting their privacy practices they are aiming to differentiate their brand and build confidence in the way they manage their private data. One good example of this is IBM that uses privacy as a brand differentiator. In a similar philosophy to IBM, the Royal Bank Financial Group [7] is using good privacy management as a tool to attract new customers, and warns that organizations that do not manage privacy will face damage to their brand.

2.3 Lawsuits

Lawsuits against organizations that violate privacy regulations or promises are becoming more common. Both Eli Lilly [6] and Toys'R Us [20] have both been hit with class action lawsuits from their customers due to violating the privacy policy that they had advertised. Other organizations that violate privacy should take this as a warning that they can fully expect to be hit with similar lawsuits unless they protect PII.

3. EXISTING PRIVACY TECHNOLOGY

As the awareness and requirements for privacy management technology has grown, a number of IT companies have begun marketing products to satisfy the demand. Some of the available products are clearly *re-branded* security technology. Although this technology might be very useful for securing data, it doesn't help an organization manage privacy. This type of technology will not be covered in this paper. This section describes the privacy technology that is designed to help manage PII. The privacy products have been classified into five categories.

3.1 Privacy Statement Creation Tools

IBM AlphaWorks [11] provides free software for creating P3P privacy statements for web sites. These P3P promises [23] are to be used by web browsers to indicate if the privacy promises of the enterprise match those set by the user in the browser. Currently only Internet Explorer V6 supports the cookie subset of the P3P language. Zero Knowledge Systems (ZKS) [13] provide a tool for creating an enterprise-internal privacy policy. This tool is part of the ZKS Enterprise Privacy Manager suite. It allows an enterprise to establish a privacy policy using a language called Privacy Rights Markup Language (PRML). Although the software allows for definition of a enterprise-internal privacy policy, it does not provide technology for enforcing the policy.

3.2 Web Site Scanning Technology

Web Site scanning technology is not new and there are a number of vendors that provide tools to scan an organization's web site. However, two of these vendors, WatchFire with their WebCPO software [24] and IDcide with their Privacy Wall software [12], have specialized in scanning web sites for privacy problems. The software *walks* an organization's web site looking for privacy compliance problems [24] such as unauthorized sharing of PII information to third parties, insecure web pages that leak data, and unsanctioned collection of personal information via server logs, web forms, cookies and web beacons.

ZKS [13] also provide a web site scanning tool, that is more limited in its function. The ZKS P3P analyzer checks a web site to ensure it has a P3P policy and to report its usage and compliance to Internet Explorer V6.

3.3 Client Privacy Software

There are a number of vendors now providing PC client software to help protect privacy while a user browsers the web. Two examples of this are McAfee's PrivacyService [15] and ZKS's Freedom Suite [13]. The aim of these products is to give a user some measure against undesirable collection of their personal data. These consumer software products are designed to give the user some management capabilities for cookies, web site advertising, form filling, logging of Internet activity, URL blocking and other functions. However, once the information is released to the enterprise, it is out of the control of these tools.

3.4 Anonymous Web Site Browsing

To enable companies and individuals to browse the web with complete anonymity, companies are providing anonymous browsing services. These companies provide a web proxy, that acts as a privacy gateway between the user's browser and the web site that is being browsed. The aim is that no information about the user or their company or organization is leaked to the web site they are browsing. This type of service is particularly useful to organizations that want to perform research without giving away any information about themselves to the organizations they are researching. Law enforcement and analyst organizations are two sectors that benefit from this type of service. Some examples of anonymous web browsing services are Anonymizer.com [2], privacy browsing service from ZKS [13] and WebVeil [25].

3.5 Privacy Certification

It is becoming more common now to see web sites branded with some type of privacy or security certification. The aim of the privacy certification is to demonstrate to users that PII information obtained by the organization is treated in an appropriate manner. The organization with the privacy certification usually agrees to periodic review by the certifying organization to ensure they are compliant.

One of the more popular privacy certifications is TRUSTe [21]. The TRUSTe "trustmark" is awarded only to sites that adhere to established privacy principles and agree to comply with ongoing TRUSTe oversight and consumer resolution protections. Note that TRUSTe does NOT provide technology to help an organization manage PII - its provides only an auditing function.

3.6 Comparison and Missing Pieces

Each of the products detailed in the above section is very specifically targeted to address a particular fraction of the PII management problem. This becomes clear in table 1 that categorizes the tools according to the OECD usage phase that they address:

- *Notice*: Before an organization collects PII, it must give notice of its intent to collect information, its privacy policies and practices, and its intended use of PII.
- *Collection*: An organization must collect information in a disciplined fashion in conformance with its privacy policies and the statements in its notice.
- *Cataloging*: An organization which collects PII should maintain a catalog of the PII in its possession to facilitate inquiries, audits, and request for access and revision.
- *Control*: An organization which collects PII should control access to and use of the information in conformance with its privacy policies and the statements in its notice.
- *Release*: An organization which collects PII must control release of the information in conformance with its privacy policies and the statements in its notice.
- *Recording*: An organization which releases or uses PII should record each release or use to facilitate inquiries, audits, and requests for access and revision.
- *Response*: An organization which collects and uses PII must respond to inquiries, complaints, and requests for access and revision in conformance with its policies and the statements in its notice.

Table 1 shows that there exists no tools for cataloging, control, record, release, and response. In other words, once information has left the hands of the consumer, it is no longer protected by any appropriate technology.

4. A NEW APPROACH FOR ENTERPRISE-WIDE PRIVACY MANAGEMENT

Existing tools for privacy management provides a patchwork where important pieces are missing. We now describe a complete framework that allows an enterprise to enforce its privacy promises and act as a custodian of their customer's PII. These building blocks provide an integrated solution for all OECD phases. Our solution is structured as follows:

1. Define an enterprise privacy policy.
2. Deploy a policy to the IT systems that contain privacy sensitive information.
3. Record consent of end users to advertised privacy policy when they submit privacy sensitive data.
4. Enforce the privacy policy and create an audit trail of access to privacy sensitive information.
5. Generate both enterprise wide and individualized reports showing accesses to privacy sensitive information and their conformance to the governing privacy policy.

4.1 Defining an Enterprise Privacy Policy

The first step in implementing a privacy management solution is to allow for the Chief Privacy Officer (CPO) or her staff to create an enterprise privacy policy. An enterprise privacy policy states the rules about the collection and use of PII. Privacy policies are defined by people who understand the business and legal environment of the organization and typically express conceptual requirements from the applicable law and business strategy. Privacy policies do not refer to specific applications or systems in the IT infrastructure, nor do they refer to specific technologies.

The exact syntax of the set of rules will depend on the language used to define the policy, however in general the policy contains the following elements:

- *Data Users*: Data Users are used to classify individuals who are accessing or receiving data. Data Users are required in a privacy context, as privacy policies will depend on the relationship between the individual requesting data and in the individual who the data is about. For example, one type of Data User might be *physician* while another might be *primary care physician*. Another distinguished data user is the *data subject*, i.e., the individual who's data has been collected. Granting rights to the data subject defines whether the data subject can access and/or update its data stored at the enterprise.

Privacy Technology	OECD Principles (from Enterprise Perspective)						
	Notice	Collect	Catalog	Control	Release	Record	Respond
Privacy Policy Creation	X						
Web Site Scanning	X	X			X[2]		
Client Privacy Software	X	X					
Anonymous Web Browsing	X	X					
Privacy Certification							
Enterprise Privacy Management	X	X	X	X	X	X	X

[2] There are scanners for web-pages but not for enterprise-internal use.

Table 1: Mapping of Privacy Product to OECD Phases

- *Operations*: Some privacy policies make distinctions about who can perform activities based on the action begin performed. For example, a policy might say that anyone in the company can *create* a customer record, but that only certain Data Users are allowed to *read* that record.
- *Data Types*: Privacy policies must define the types of data which the enterprise will be holding. Typically, the Data Types used in privacy policies are high-level descriptions of data, such as *customer contact information*. Detailed, low-level descriptions are not typically required in privacy policies.
- *Purposes*: Data access requests are made for a specific purpose or purposes. This represents how the data is going to be used by the recipient. For example, the data may be used for *marketing* or *fulfillment* of the individual's order.
- *Conditions*: Rules can be qualified based upon additional conditions. Often, legislation or privacy policies make statements based on specified conditions. For example, COPPA [8] imposes requirements on data received from persons less than 13 years of age. Another common condition is that the user must have consented before PII can be used for a particular purpose.
- *Obligations*: A privacy policy may also state that when a certain access is allowed, the enterprise must take some additional steps. An example is that all accesses against a certain type of data for a given purpose must be *logged*. Another might be that PII must be *deleted* if its owner has not performed business with the enterprise for one year.

The elements are then used as the terminology to express privacy rules expressing what requested data accesses are allowed or denied, and under what conditions:

```
ALLOW [Data User]
to perform [Operation] on [Data Type]
for [Purpose] provided [Condition].
Carry out [Obligation].
```

Note that a goal is that enforcing such a formalization should reflect the legal regulations and the expectations of the consumers that gave consent to a particular privacy statement. This requires that the terms are narrow and well-defined. Furthermore, the policy needs to be designed with the individuals expectations in mind [1]: A permission to send product information, e.g., implies a condition that the number of mails is small.

4.2 Deploying a Policy to the IT Systems

After the CPO or an equivalent person has created an enterprise privacy policy, the IT staff can now deploy this to the actual IT systems within the enterprise. Deploying a policy consists of three steps:

1. Mapping the Data Types defined in the privacy policy to the PII that is stored in the IT systems.
2. Mapping the Data Users defined in the privacy policy to enterprise roles that are defined in the IT systems.
3. Mapping the tasks that IT systems and applications perform into policy defined business purposes.

These mapping tables allow for the rules engine to *resolve* a physical data access on an IT system with the privacy policy that has been defined.

Consider data that is stored in a database. In this case, the *customer* database, might have a table called *address*, with a column called *home_phone_number*. The IT staff may create a map that would associate this with a Data Type called *Sensitive_Address_Information*. Hence, when access to this column is made, the privacy enforcement system can quickly resolve this physical data to the privacy policy Data Type, and find the subset of rules that apply to this Data Type. An access decision can then be made based on the privacy rules and user consents.

Note that multiple storage locations can be tagged with the same Data Type and one storage location can be tagged with multiple Data Types.

A similar process occurs for mapping enterprise roles to the Data Users defined in the privacy policies. So for example, an enterprise role of *Bank Teller*, may map to a Data User of *Bank Officer*.

4.3 Recording Consent of End Users

At the heart of managing PII is to ensure that a user has consented to use of their data before its used within the enterprise. The user should explicitly consent to the privacy policy advertised, and to each and every purpose of use in the enterprise. An enterprise should not accept any PII until the user has consented to the privacy policy in place and consented (positively or negatively) to use of the data for each purpose. Besides recording the collected data, this requires the following privacy management data:

- An identifier of the person whose data is being submitted.
- The PII types being submitted.
- The mapping of the collected data onto the PII types.
- The storage of user consents.
- The time of the data submission.
- The applicable version of the privacy policy.

This comprises all information necessary to govern all future usage of the data. An important point to note, is that the data is submitted under a particular privacy policy, and should be *linked* to that policy. We call this approach to managing PII "the sticky policy paradigm". If the enterprise's privacy policy is updated (which it will in time), it is important that the user's data is managed under the policy at consent time, and not to this new policy. Only if the user explicitly consents to the new policy should that data be treated under this new policy.

4.4 Enforce the Privacy Policy and Create an Audit Trail of Access

The other key task is to watch for applications accessing private data in a protected system. This requires identifying whose data is being accessed, its PII type, who is accessing the data and the time the access occurred. This information is used to retrieve the submission record corresponding to the data that is being accessed, the governing privacy policy and the user's consents, and finally to decide whether access shall be granted or not.

For efficiency reasons, this can be done in two modes:

1. *Real-time Privacy Enforcement*: The privacy policy and user consents are checked in real time. If the access is denied, then the operation fails.
2. *Near-time Conformance Checking*: In this mode the data accesses are not blocked. The data access is always allowed to complete. An audit record is created and evaluated. If the access should have been denied then an alert is raised with an administrator.

Note that one can partially use existing access control concepts [17] to decide whether access shall be allowed or not. For privacy, however, this decision often depend on the purpose for which an access is requested. Such purpose-binding is not provided by standard access control systems. In this case, privacy-specific access control systems [14, 9] are required instead.

4.5 Generate Both Enterprise Wide and Individual Reports

Being able to report on activities relating to PII is an essential part of privacy management. This requires generation of reports both at an enterprise-wide perspective and and at an individual perspective. For example, an individual may make a request to an organization, "What data do you have stored about me, who has been accessing it and for what purpose?". An auditor may ask "Please show me a report showing any PII accesses that were outside of privacy policy or user consents". Because the privacy management system has kept very detailed audit records of submissions and accesses, both of these questions can be answered.

4.6 Provide Privacy Services for the Individual

The enterprise needs to provide privacy management services to the individual. These services provide a one-stop user-interface to the privacy management systems of the enterprise. These include services

- to review and/or update of the applicable privacy policy and the given consent,
- to review and/or update of the stored data,
- to distribute privacy notifications, and
- to review the privacy reports generated in Section 4.5,
- services and business processes to recover from privacy violations for near-time conformance checking.

The look and feel of these services should resemble the business and its applications. As a consequences, one can only provide a tool-box for privacy services. The actual privacy services are then implemented by the applications of the business. Services for reviewing data and consent, for example, can be tightly integrated into the self-management of a customer's account. In addition, an enterprise needs to establish processes for managing customer complaints. Examples are to examine alleged privacy violations and processes for recovering from privacy violations that were reported by near-time conformance checks.

5. AN ARCHITECTURE FOR ENTERPRISE-WIDE PRIVACY ENFORCEMENT

Figure 1 shows one architecture for implementing Privacy Management services within an enterprise. On the left hand side of the figure is a client of the enterprise (say an Internet user) that submits PII to the enterprise. On the right hand side is an enterprise employee that wants to access the PII (for order fulfillment, marketing or other purposes).

The core management component is a Privacy Management Server. This is the heart of our privacy management technology and provides the rules processing engine that authorizes requests, raises alerts and produces the audit logs.

The core enforcement components are Privacy Monitors that protects particular resources. They observe and protect data going in and out of monitored systems that store PII. A

Monitor may be a piece of software that intercepts traffic on the wire, or may be built into an application using a Monitor SDK.[3]

The privacy policies are created by our policy editor tool. These can be placed on a web site and are also used internally by the Privacy Management server.

When a user (shown as Data Subject) submits PII to the enterprise the submission Monitor tracks the PII, the user's consents to use of the data, and the privacy policy in place at time of submission.

When an internal employee (shown as Data User) tries to access the data an enforcement Monitor needs to see if the access corresponds to both the enterprise privacy policy and the user's consents.

Privacy services (see Section 4.6) will usually run on the web application server for direct use use by the individual. Highly sensitive parts of it may only be implemented as business applications. E.g., reviewing usage logs may be restricted to the chief privacy officer after being authorized by the individual. Correcting customer data may be restricted to help-line employees that can perform the required consistency checks. Our architecture focuses on enterprise infrastructure, i.e., we do non address the design of these privacy services and other privacy-specific aspects of human-computer interaction (see, e.g., [1] for a model of user-perception of privacy in multimedia systems).

6. CONCLUSIONS

Privacy Management is not only a security problem. Although it requires secure systems as a prerequisite as well as some security technology for access enforcement and audit trails, it is closer to a data management problem.

We have described a new approach that enables enterprises to act as a custodian of their customer's personal data. Enterprises that value customer relationships more than their collected data can use this technology to enforce the privacy promises they make and to enable their customers to retain control over their data.

This technology addresses most aspects of privacy management for collected customer data and is a candidate for replacing the current patchwork of partial solutions by a consistent solution that covers the complete picture ranging from creating and managing privacy policies, PII submission monitoring, user consent management, privacy enforcement, reporting and auditing.

Unfortunately, our technology is limited to managing and protecting collected customer data. It does not address all potential privacy problems. Some issues that are still open are protecting data that changes its sensitivity while being stored, or privacy-invasive deductions and statistics based on data that a data user can access.

[3] We call such applications with an integrated monitor "privacy-aware applications" since they ask the Privacy Management Server for authorization before actually processing their data.

Acknowledgments

We thank Günter Karjoth for contributions on enterprise privacy policies. In addition, we would like to thank our reviewers for constructive comments that helped us to improve the paper. Parts of this work have been funded by the IBM Privacy Institute (see www.research.ibm.com/privacy).

7. REFERENCES

[1] Anne Adams and Martina Angela Sasse. Privacy in multimedia communications : Protecting users, not just data. In A. Blandford and J. Vanderdonkt, editors, *People and Computers XV - Interaction without frontiers. Joint Proceedings of HCI2001 and ICM2001*, pages 49–64. Springer-Verlag, Berlin, 2001.

[2] Anonymizer.com. Anonymous Web Browsing Service. www.anonymizer.com.

[3] Australia. Privacy Act 1988, 1988. Available at www.privacy.gov.au/act/index.html.

[4] Canada. The Personal Information Protection and Electronics Document Act: Bill C6. Available at www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_3/C-%6_cover-E.html.

[5] Federal Trade Commission. FTC Announces Settlement With Bankrupt Website, July 2001. www.ftp.gov/opa/2000/07/toysmart2.htm.

[6] Federal Trade Commission. Eli Lilly Settles FTC Charges Concerning Security Breach, January 18 2002. Available at www.ftc.gov/opa/2002/01/elililly.htm.

[7] ComputerWorld. Profitable Privacy, February 2002. Available at www.computerworld.com/storyba/0,4125,NAV47_STO68354,00.html.

[8] COPPA. Children's Online Privacy Protection Act of 1998 (COPPA), October 1998. Available at www.cdt.org/legislation/105th/privacy/coppa.html.

[9] Simone Fischer-Hübner. *IT-Security and Privacy : Design and Use of Privacy-Enhancing Security Mechanisms.* Number 1958 in Lecture Notes in Computer Science (LNCS). Springer Verlag, Berlin, 2001.

[10] Organisation for Economic Co-operation and Development. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980. Available at webnet1.oecd.org/oecd/pages/home/displaygeneral/0,3380,EN-document-43-1-no-24-10255-43---,FF.html.

[11] IBM. IBM Alphaworks P3P Policy Editor. Available at www.alphaworks.ibm.com/tech/p3peditor.

[12] iDcide. iDcide Privacy Wall Privacy Technology. Available at www.idcide.com.

[13] Zero Knowledge Systems Inc. Enterprise Privacy Manager, P3P Analyzer, Freedom Suite and Private Browsing Service. www.zeroknowledge.com.

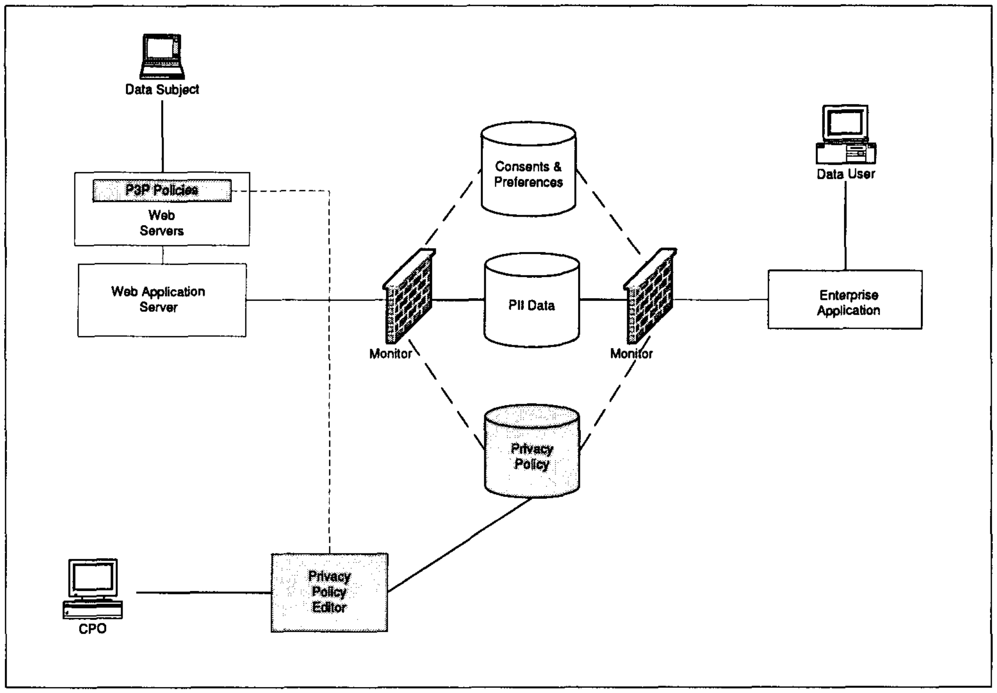

Figure 1: Architecture for Enterprise Privacy Management and Enforcement

[14] G. Karjoth, M. Schunter, and M. Waidner. The Platform For Enterprise Privacy Practices – Privacy-enabled Management Of Customer Data. In *Proceedings of the Privacy Enhancing Technologies Conference*, San Francisco, CA, April 14-15 2002.

[15] McAfee. PrivacyService. `www.mcafee.com`.

[16] Forrester Research. Privacy Concerns Cost e-Commerce $15 Billion, September 2001. `www.forrester.com`.

[17] R. Sandhu and P. Samarati. Access control: Principles and practice. *IEEE Communications*, 32(9):40–48, 1994.

[18] HIPAA States. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), October 1998. Available at `www.hcfa.gov/hipaa/hipaahm.html`.

[19] United States. Gramm-Leach-Bliley Act: Financial Privacy and Pretexting, November 12 1999. Available at `www.ftc.gov/privacy/glbact/glboutline.htm`.

[20] E-Commerce Times. Toys 'R' Us Sued for Net Privacy Violations, July 2001. `www.ecommercetimes.com/perl/story/3957.html`.

[21] TRUSTe. Privacy Certification. Available at `www.truste.com`.

[22] European Union. The European Union Directive 95/46/EC: On The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data, February 20 1995. Available at `www.privacy.org/pi/intl_orgs/ec/eudp.html`.

[23] W3C. Platform for Privacy Preferences. Available at `www.w3.org/P3P`.

[24] WatchFire. WatchFire WebCPO: WebSite Privacy Management Software. Available at `www.watchfire.com/solutions/webcpo.asp`.

[25] WebVeil. WebVeil Web Proxy. `www.webveil.com`.

APPENDIX

A. OECD PRIVACY PRINCIPLES

The OECD guidelines for the protection of privacy can be found in [10]. The core of the OECD guidelines are the eight privacy principles, and it is managing PII to these principles, that is at the core of the proposal in this paper for privacy management technology.

1. *Collection Limitation Principle*: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. *Data Quality Principle*: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and be kept up-to-date.
3. *Purpose Specification Principle*: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. *Use Limitation Principle*: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except a) with the consent of the data subject or b) by the authority of the law.
5. *Security Safeguards Principle*: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6. *Openness Principle*: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. *Individual Participation Principle*: An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time, at a charge, if any, that is not excessive, in a reasonable manner, and in a form that is readily intelligible to him; c) to be given reasons if a request made under a) or b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed, or amended.
8. *Accountability Principle*: A data controller should be accountable for complying with measures which give effect to the principles stated above.