Dealing with Privacy Obligations in Enterprises[±]

Marco Casassa Mont
Trusted Systems Laboratory
HP Laboratories Bristol
HPL-2004-109
June 30, 2004*

privacy, privacy obligations, policies, privacy obligation management, enforcement, accountability, trusted system, identity management

This paper focuses on the problem of dealing with privacy obligations in enterprises. Privacy obligations dictate expected behaviours, tasks and constraints that must be satisfied when handling personal and confidential data. This includes being compliant with data retention policies and satisfying constraints dictated by customers' opt-in and opt-out choices. It is important for enterprises to address this problem to preserve their reputation and brand and be compliant with legislation and customers' requirements. This paper describes important related issues and requirements to be kept into account, including dealing with transactional, ongoing and long-term obligations. Technical work has already been done for the management of obligations subordinated to authorization aspects and simple obligations for data retention: however, dealing with ongoing and long-term aspects of obligations is still a green field and open to research. We introduce and describe a trusted system, currently under research and development at HP Labs, dealing with the monitoring, enforcement and tracking of privacy obligations: this system will support the strong association of privacy obligations to data, accountability management and users' involvement.

* Internal Accession Date Only
[±] ISSE 2004, Berlin, 28-30 September 2004 Approved for External Publication

Dealing with Privacy Obligations in Enterprises

Marco Casassa Mont

Hewlett-Packard Laboratories
Filton Road, Stoke Gifford, Bristol, UK
marco.casassa-mont@hp.com

Abstract

This paper focuses on the problem of dealing with privacy obligations in enterprises. Privacy obligations dictate expected behaviours, tasks and constraints that must be satisfied when handling personal and confidential data. This includes being compliant with data retention policies and satisfying constraints dictated by customers' opt-in and opt-out choices.
It is important for enterprises to address this problem to preserve their reputation and brand and be compliant with legislation and customers' requirements. This paper describes important related issues and requirements to be kept into account, including dealing with transactional, ongoing and long-term obligations.
Technical work has already been done for the management of obligations subordinated to authorization aspects and simple obligations for data retention: however, dealing with ongoing and long-term aspects of obligations is still a green field and open to research. We introduce and describe a trusted system, currently under research and development at HP Labs, dealing with the monitoring, enforcement and tracking of privacy obligations: this system will support the strong association of privacy obligations to data, accountability management and users' involvement.

1 Introduction

Enterprises store, manage and process large amounts of personal and confidential data related to their employees, customers and partners. On one hand, this information is fundamental to enable their business processes, interactions and transactions. On the other hand, personal data should be accessed and used only for the purposes for which it has been disclosed and with the consent of the data owners or data subjects. Enterprises increasingly recognise that dealing correctly and honestly with privacy matters can have a beneficial return in terms of branding, trust, customers' satisfaction and business opportunities.

When processing, using and transmitting confidential data, enterprises must be compliant with privacy laws. A lot of work has been done in terms of privacy legislation often driven by local or geographical needs. This includes European Community data protection privacy laws, various US privacy laws and more specific national privacy initiatives [Laur03]. Guidelines are also available on the protection of privacy and flows of personal data, including OECD guidelines [Oecd80], that describe concepts such as collection limitation, data quality and purpose specification principles and online privacy policies [Priv04]. Large enterprises that are geographically distributed across different nations might need to comply with different privacy laws.

Privacy policies can be used to represent and describe privacy laws, guidelines and privacy statements. Privacy policies, at the very base, express rights, permissions and obligations, usually in natural language that needs to be interpreted and understood by people.

This paper focuses on technical aspects related to the management and enforcement of privacy obligations as part of the wider problem of dealing with privacy policies.

In general privacy policies can be hard to enforce via IT solutions. The enforcement of privacy rights, permissions and obligations related to confidential and personal data requires the mapping of these concepts (that are most of the time abstract and based on high-level principles) into rules, constraints and access control, the meaning of which must be unambiguous so that it can be deployed and enforced by software solutions. Dealing with this still requires that the entities involved in the management of confidential and personal data follow best practices and good behaviours. However, being able to automate aspects of the enforcement of privacy policies and reduce the involved costs is important for enterprises.

Advancements in this direction have already been made when dealing with the (technological) enforcement of privacy permissions. Extended access control and authorization mechanisms have been built to check privacy permissions against users' rights, the purpose of the confidential information (that needs to be accessed) and the declared intents. This is the case, for example, of web transactions and interactions or applications/services within organizations that need to access and manipulate confidential data for business reasons.

More complex is the case of dealing with privacy obligations. They might include the deletion of confidential data after a predefined (potentially very long) period of time, periodic notifications and request for authorization to data owners or data subjects, fulfilment of opt-in/opt-out choices made by data owners, ongoing compliance with laws' obligations and internal guidelines. The events that trigger the fulfilment of privacy obligations can be completely orthogonal to the ones relevant for privacy permissions. Privacy obligations can have ongoing aspects that need to be monitored and satisfied over a long period of time. These tasks are challenging for enterprises because of the need for specific IT infrastructures and processes able to manipulate confidential data as dictated by privacy obligations.

The management and enforcement of privacy obligations, as first class citizens, is still a green field and open to research. In this paper we analyse some of the related issues, describe possible technical approaches to move towards a more explicit management and enforcement of privacy obligations and introduce a trusted system, dealing with obligations, that is currently under research at HP Labs.

2 Privacy Obligations

Privacy obligations define and describe expected behaviours and constraints to be satisfied by enterprises when dealing with confidential and personal data. Enterprises need to put in place underlying IT infrastructures, processes and mechanisms to be compliant with these obligations. This can be a challenging task due to the fact that privacy obligations can differ quite substantially depending on:

- **Level of refinement**: abstract vs. refined;
- **Enforcement timeframe**: short-term vs. long-term;
- **Expected enforcement actions**: one time vs. ongoing actions.

Privacy obligations can be very abstract, for example: "every financial institution has an affirmative and continuing obligation to respect customer privacy and protect the security and

confidentiality of customer information" - Gramm-Leach-Bliley Act (1999). More refined privacy obligations can be expressed in terms of notice requirements, opt-out options, limits on reuse of information and information sharing for marketing purposes. At the other extreme, privacy obligations can dictate very specific requirements. This is the case where data retention has to be enforced for a long period of time or data is temporarily stored by organisations: privacy obligations can require that personal data must be deleted after a predefined number of years, e.g. 30 years (i.e. long-term commitment) - or in a few days if user's consent is not granted (i.e. short-term commitment).

The topic related to "privacy obligations" is complex: exploring all the possible implications and involved aspects goes far beyond the purpose of this paper. In this paper we focus on enforceable privacy obligations for personal and confidential data stored and managed by enterprises. In general different aspects need to be kept in account when dealing with these obligations:

- **The period of validity of obligations**;
- **The degree of enforceability of obligations**;
- **The events that trigger the need to fulfil obligations**;
- **The target (involved data) of an obligation**;
- **The actions that need to be executed to enforce an obligations;**
- **The entities that are responsible for enforcing obligations;**
- **Accountability criteria**;
- **Exceptions**.

It is important to clearly specify who is accountable for managing and enforcing privacy obligations. Exceptions need to be handled and criteria introduced (such as imposing strong auditing) to avoid abuses. In this paper we specifically explore the requirements and issues related to the management and enforcement of three core categories of privacy obligations: (1) long-term privacy obligations, (2) short-term privacy obligations, (3) ongoing privacy obligations. Table 1 shows examples of these types of obligations along with related events and actions.

Table 1: Types of privacy obligations and examples of related events and actions.

<table>
<tr><th colspan="4">Long-term Privacy Obligations</th></tr>
<tr><th colspan="2">Events Triggering Obligations</th><th colspan="2">Actions Dictated by Obligations</th></tr>
<tr><td>Time-driven</td><td rowspan="2">1. at a specific date and time (e.g. 1:00am 01-Jan-2005)
2. after a certain period of time (e.g. 1 hour, 3 days, 5 minutes)
3. after the data has being used for a certain number of times (e.g. after being used twice) in a specific time-frame</td><td>Delete/ Update</td><td>1. delete all confidential data of a given data subject
2. partially delete data (e.g. delete only the credit card number)
3. replace data with an updated set of data (e.g. update subject's address)</td></tr>
<tr><td>Driven by Usage and Counters</td><td>Hide/ Unhide</td><td>1. hide (encrypt) all data of a subject from any access
2. hide a part of this data from any access
3. unhide all data
4. unhide a part of the data</td></tr>
</table>

<table>
<tr><th colspan="4">Ongoing Privacy Obligations</th></tr>
<tr><th colspan="2">Events Triggering Obligations</th><th colspan="2">Actions Dictated by Obligations</th></tr>
<tr><td>Time-driven</td><td>1. periodically (e.g. every month)</td><td></td><td>1. send a report to a subject containing the status of their data and their opt-in/opt-out options (e.g. number of times being used, who has tried to access)
2. tell the subject what data he/she has provided
3. get updated data from subject
4. audit the logs, report any improper use of the data</td></tr>
<tr><td rowspan="4">Driven by Contextual Events</td><td rowspan="4">1. when the data being used
2. when the data being transferred
3. when the data being deleted
4. a particular party/parties try to access
5. data is being used for certain purpose (e.g. send advertisement)
6. a set of data is going to be retrieved together
7. any action predefined by the data subject</td><td>Notify</td><td>1. notify the subject</td></tr>
<tr><td>Log</td><td>1. take logs</td></tr>
<tr><td>Access</td><td>1. default allow/disallow all access
2. allow
3. disallow</td></tr>
<tr><td>Consult</td><td>1. get authorization from data subject
2. get authorization from third party
3. check according to certain condition made by the user</td></tr>
<tr><td>Others</td><td>1. when the privacy policies changed</td><td></td><td>1. Stop access to the data
2. update obligation</td></tr>
<tr><th colspan="4">Short-term and Transactional Privacy Obligations</th></tr>
<tr><td colspan="4">Obligations might need to be dictated by a transaction or an interaction. The actions specified by these obligations might need to be immediately fulfilled. These actions can be the same as the ones specified by long-term and on-going obligations.</td></tr>
</table>

3 Important Issues and Requirements

Important issues and requirements need to be considered when dealing with the management and enforcement of privacy obligations:

- **Representation of privacy obligations**: privacy obligations need to be represented with an appropriate language to describe which data is affected by an obligation, the events and conditions that trigger the fulfilment of the obligation, actions to be carried on, which entities are responsible and accountable for their enforcement;
- **Association of obligations to data**: the association of privacy obligations to the targeted confidential data must not be easy to be broken. This aspect is particularly challenging in dynamic environments where confidential data can be moved around or sent to other parties;
- **Mapping obligations into actions**: when possible, actions dictated by obligations must be expressed in a way that can be programmatically enforced; otherwise, they should trigger related processes and workflows involving the human intervention and clearly state responsibilities;

- **Compliance of refined obligations to high-level policies**: the mapping of high level policies to refined privacy obligations (and the affected data) should be managed explicitly and tools built to spot potential inconsistencies and dependencies;
- **Tracking the evolutions of obligation policies**: obligation policies can be carried on over long periods of time and are subject to changes. Changes need to be tracked and obligations versioned, for accountability reasons and to deal with the evolution of the contexts and frameworks where these obligations apply;
- **Dealing with long-term obligation aspects**: long-term obligations have implications on the longevity and survivability of related processes and the involved data. Solutions needs to be build to last over a long period of time;
- **Accountability management**: as anticipated before, accountability management is fundamental to ensure that the enforcement of privacy obligations is carried on with clear responsibilities of the involved parties. This introduces requirements in terms of auditing, tracking of obligations and their monitoring;
- **Monitoring obligations**: the fulfilment of obligations must be monitored and checked against expected situations and behaviours. Despite good intents and enforcement mechanisms, it can always happen that the fulfilment of obligations is omitted. Monitoring mechanisms must be orthogonal to the enforcement mechanisms. Problems need to be notified to the responsible entities;
- **User involvement and awareness**: Users should have visibility of which obligations an organisation has with them. Tools should be provided to uses to allow them to monitor their fulfilment and directly manage their privacy obligations;
- **Complexity and cost of instrumenting applications and services**: the enforcement and monitoring of obligation policies can have an impact on the involved applications and services, both in terms of their instrumentation and development costs. A privacy obligation framework should reduce to the minimum this impact.

The management and enforcement of privacy obligations can be reasonably easy when the events that trigger them are well defined and easy to capture, for example they depend on time or known transactions or interactions. More complex is the case of privacy obligations related to ongoing obligations, triggered by the occurrence of events and conditions non-necessarily related to time or known transactions (for example dictated by laws, user's requests, etc.).

4 Addressed Problems

In this paper we address the problem of dealing with the explicit management of privacy obligations, on an ongoing basis, including short-term and long-term privacy obligations. This includes dealing with the monitoring, enforcement, and tracking of privacy obligations. We also want to address the related problems of managing the strong association of privacy obligations to data, enforce accountability and provide more transparency to users.

We believe that the reliable and verifiable management of personal data, in accordance with legal requirements and the policies of the data subjects/owners, is more easily achieved if it is controlled by privacy specific middleware rather than by application-level code. After all, the driving force behind any application solution is the set of business processes for which it is designed, not the privacy management aspects of the personal data it processes. The use of privacy management middleware allows a common (as supposed to piecemeal) approach to privacy issues to be taken, thereby creating trusted systems.

Work has already been done to address some of these issues, in particular related to the representation of privacy policies (and obligations), their enforcement in transactional and interaction-driven contexts and the management of simple long-term aspects of obligations for data retention. In many cases, though, obligation policies are considered as second-class entities the enforcement of which is subordinated to other aspects of privacy policies, such as privacy permissions.

A more explicit and comprehensive approach to privacy obligations is required. We aim at researching and building a trusted system where privacy obligations are considered as first-class "citizens" and can be managed without their subordination to other aspects such the management of privacy permissions or access control/authorization.

5 Related Work

Relevant work in the space of privacy management for enterprises is described in [KaSc02, KaSW02a, ScAs02, KaSW02b]. Enterprise Privacy Architecture is introduced and described in [KaSW02b], encompassing a policy management system, a privacy enforcement system and an audit console. Paper [ScAs02] introduces more architectural details along with an interpretation of the concept of privacy obligations. This concept is framed in the context of privacy rules defined for authorization purposes. This approach is further refined and described in the Enterprise Privacy Authorization Language (EPAL) specification [Epal04].

The above work makes important advancements in exploring and addressing the problem of privacy management in enterprises but it only considers the authorization and access control perspective as the driver for their representation, management and enforcement. It has still to be fully demonstrated that privacy obligations can be managed at their best from an authorization-based perspective. Privacy obligations can include aspects that are not really driven by authorization aspects, such as dealing with the deletion of confidential data at a specific date/event, periodically providing notifications to subjects about stored confidential data, dealing with ongoing requests dictated by subjects or laws. We believe that the representation, management and enforcement of privacy rights, obligations and permissions should be addressed without imposing any specific or dominant perspective.

In our proposed approach (described in the next sections) obligation policies are first-class "citizens" that are explicitly managed. Even if our architecture has high-level commonalities with the architecture described in [KaSc02, KaSW02a, ScAs02, KaSW02b] we further refine the concept of obligations and we introduce the concept of obligation versioning and tracking. We also split the enforcement mechanisms in two parts by including a scheduling mechanisms and an obligation enforcer where the obligations actions are carried out by flexible workflow processes that allows both automation and the involvement of people.

Mechanisms to deal with (privacy) obligations have already been implemented in products, in particular for data retention [Ibmt04] and in a variety of document management systems. Nevertheless, these approaches are very specific; they are focused on particular domains and handle simple obligation policies. Our work wants to push the barrier even further to create an obligation management framework that can be leveraged in multiple contexts, for different purposes.

A lot of work has been done in representing privacy policies, including obligations such as [Epal04, BJSW02, DDLS01]. Work describing the monitoring of obligations in policy management is described in [DDLS01]. Relevant work on mechanisms to associate policies to data is described in [KaSc02, KaSW02a, ScAs02, KaSW02b, CaPB03, AKSX02]. Each

mechanism has pros and cons in terms of the implications for existing enterprise applications, services and data repositories. We can leverage aspects of this work, in particular [CaPB03] to provide a stronger association of obligation policies to confidential data.

6 Technical Details

This section provides technical details about the approaches and solutions under exploration at HP Labs to address the problems stated in section 4. Figure 1 shows a high-level architecture of a trusted system providing an explicit management of privacy obligations:

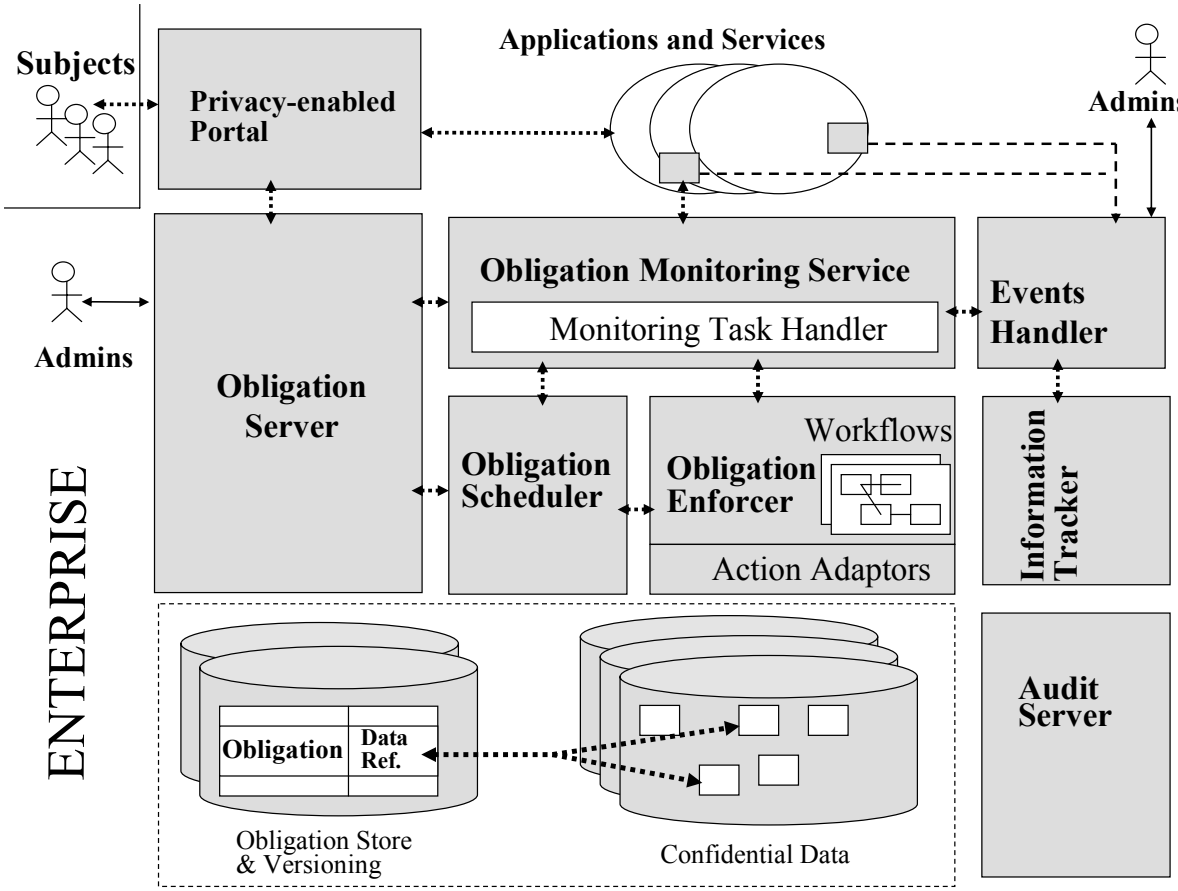

Fig. 1: High-level Architecture

The obligation management system consists of:

- **Obligation Server**: it deals with the authoring, management and storage of obligations. It explicitly manages the association of privacy obligations to confidential data and their tracking and versioning. It pushes active obligations (i.e. obligations to be fulfilled) to the "obligation scheduler". One or more obligation servers can be deployed (and synchronised), depending on needs;
- **Obligation Store and Versioning**: it stores obligations and their mapping to confidential data. Multiple versions of obligations are also stored in this system;
- **Obligation Scheduler**: it is the component that knows which obligations are active, ongoing obligation deadlines, relevant events and their association to obligations. When events/conditions trigger the fulfilment of one or more obligations, this component activate the correspondent "workflow processes" of the "obligation enforcer" that will deal with the enforcement of the obligation.

- **Obligation Enforcer**: it is a workflow system containing workflow processes describing how to enforce one or more obligations. The enforcement can be automatic and/or could require human intervention, depending on the nature of the obligation;
- **Events Handler**: it is the component in charge of monitoring and detecting relevant events for privacy obligations and sending them to the obligation scheduler. The detection of events can happen via instrumented application/services. They can also be directly generated by users, administrators, the "obligation monitoring service" and the information tracker;
- **Obligation Monitoring Service**: it is the component, orthogonal to the scheduling and enforcement systems that monitors active obligations and if they have been enforced by analysing and checking for the effects of their actions;
- **Information tracker**: it is a component that focuses on intercepting events generated by data repositories, databases and file systems containing confidential data and providing this information to the event handler. It is aware of the location of confidential data (as described by the obligation policies) and checks for movements and changes happening to this data;
- **Audit Server**: it audits the relevant events and information generated by the overall system components and involved applications/services.

In our model, privacy obligations contain the description of relevant events/conditions, actions, targeted data (i.e. links to related confidential data) and accountable/responsible entities.

Issues arise when the overall environment is dynamic and data can be moved around: in this case the association of data to obligations policies can be broken or be left in an inconsistent state.

To address this issue we are exploring a variant of the architecture shown in figure 1, where stronger mechanisms are introduces to manage the association of obligations to data. Confidential data is obfuscated and strongly associated to privacy obligations by using cryptographic and enveloping techniques. A key management system is introduced to deal with this task as a subsystem of the Obligation Server.

Data envelopes are encrypted with the public key [HFPS99] of the key management system. The triple consisting of <*obligation policy, encrypted envelope, obfuscated data*> is stored as a replacement of the original data. The obligation policy must contain a reference to the competent Obligation Server but it can omit the reference to confidential data, as the policy is now directly associated to this data. In this way, the encrypted confidential data can be moved around and transmitted to other parties without an upfront control. The receiving party has to interact with the Obligation Server to decrypt the data: this allows the system to track and audit where the data is, check for relevant obligations and update its obligation store. The basic principles and additional details on how this approach can be implemented are described in [CaPB03, Casa04].

7 Discussion

Because of its nature, the system described in this paper has to be considered as a trusted system. It must be deployed by keeping in mind good security practices, especially for the platforms that will host our system components. Its core components are critical hence they require to be secured accordingly. Additional trust and accountability can be added by harden-

ing the audit server and involving trusted third parties in the monitoring of the enforcement of obligation policies.

This system centralises the storage of privacy obligations along with their management. It can support the management of versions of privacy obligations over time and enable the tracking of their changes (and related applicability contexts) for auditing and accountability reasons. We are exploring how these aspects can be distributed to avoid potential bottlenecks and central points of failure, without compromising the overall security and integrity of the system.

The approach described in figure 1 is almost transparent to the data affected by privacy obligations. The second approach, involving cryptographic mechanisms, requires changes to data repositories to accommodate encrypted data. In both cases, applications and services might require some instrumentation, if applications/service-based events need to be detected. We are currently investigating how a hybrid solution can be used to accommodate different needs and requirements.

Our system explicitly focuses on the management and enforcement of obligations: this does not imply that it has to happen independently by other privacy aspects, such as permissions. It should be considered as a sub-system of a more comprehensive privacy management framework.

When dealing with long-term privacy obligations it is also important to ensure the reliability and longevity of the platforms running our system components and the survivability of the involved data and obligations. Work has already been done in this space, including [Ande96, EFL+98, KBC+00, Neum99, WBS+00], and can be leveraged.

8 Current and Future Work

An initial prototype has been implemented, consisting of four core components – obligation server, obligation scheduler, obligation enforcer and obligation monitor - and deployed within an enterprise environment. Figure 2 shows the architecture of the implemented prototype.

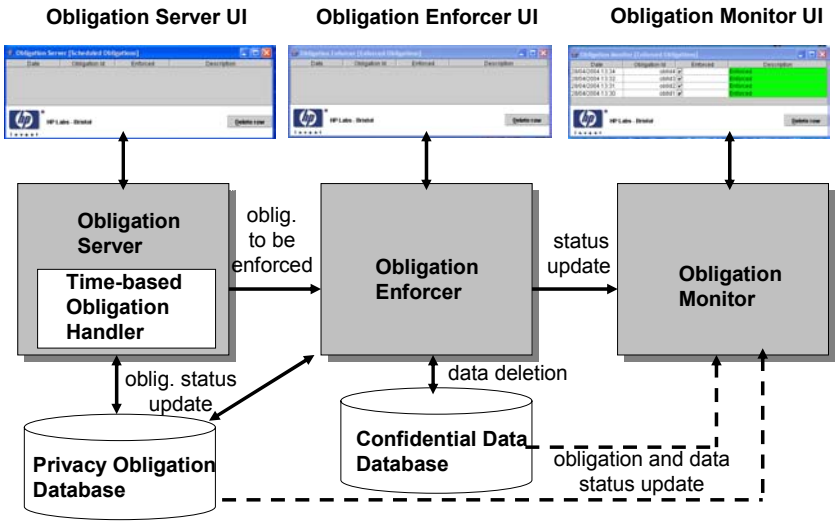

Fig. 2: Architecture of Current Prototype

Privacy obligation policies have been represented by using an XML format to allow their future extensions. At the moment two categories of obligations are supported: long-term and short-term/transactional obligations. Modules to support ongoing obligations are under development. Current privacy obligations can be used to describe time-based events and actions requiring deletion or partial deletion of personal data stored in relational databases. The goal of this prototype is to show the feasibility of our ideas: the functionalities described in section 6 will be incrementally implemented in the next few months.

Our work and research is definitely in progress: technical aspects need to be further refined and investigated, especially the ones related to the life-cycle management of privacy obligations and events. The overall implications on enterprise applications and services need to be fully understood. Tools and mechanisms to address the compliance of refined obligations to high-level policies are also under investigation.

9 Conclusion

The management of privacy obligations is important for enterprises to preserve their reputation and brand, be compliant with legislation and customers' requirements and increase business opportunities. This paper describes important issues that need to be kept into account by enterprises when dealing with privacy obligations. In our vision privacy obligations (as well as for other privacy aspects, including rights and permissions) need to be considered as first-class "citizens" within privacy management frameworks.

We introduce a technical approach to deal with the explicit management of privacy obligations including transactional/short-term, long-term and ongoing privacy obligations. We provide a high-level description of a trusted system and its components dealing with the monitoring, enforcement, and tracking of privacy obligations. We discuss the problem of strongly associating privacy obligations to confidential data in dynamic environment and dealing with accountability management.

Our research and work is in progress. A prototype has been developed to test our ideas. Additional functionalities will be added in the next months.

Acknowledgements

A special thank to Kwok Nga (Annie) Chan, for the material used in table 1 and Pete Bramhall for his feedback and inputs to this paper.

Index

Privacy, Privacy Obligations, Policies, Privacy Obligation Management, Enforcement, Accountability, Trusted System, Identity Management

References

[Laur03] Laurant, C., Privacy International: Privacy and Human Rights 2003: an International Survey of Privacy Laws and Developments, Electronic Privacy Information Center (EPIC), Privacy International. http://www.privacyinternational.org/survey/phr2003/, 2003

[Oecd80] OECD: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. http://www1.oecd.org/publications/e-book/9302011E.PDF, 1980

[Priv04] Online Privacy Alliance: Guidelines for Online Privacy Policies. http://www.privacyalliance.org/, Online Privacy Alliance, 2004

[KaSc02] Karjoth, G., Schunter, M.: A Privacy Policy Model for Enterprises. IBM Research, Zurich. 15th IEEE Computer Foundations Workshop, 2002

[KaSW02a] Karjoth, G., Schunter, M., Waidner, M.: Platform for Enterprise Privacy Practices: Privacy-enabled Management of Customer Data. 2nd Workshop on Privacy Enhancing Technologies, Lecture Notes in Computer Science, Springer Verlang, 2002

[ScAs02] Schunter, M., Ashley, P.: The Platform for Enterprise Privacy Practices. IBM Zurich Research Laboratory, 2002

[KaSW02b] Karjoth, G., Schunter, M., Waidner, M.: Privacy-enabled Services for Enterprises. IBM Zurich Research Laboratory, TrustBus 2002, 2002

[Epal04] IBM: The Enterprise Privacy Authorization Language (EPAL), EPAL 1.1 specification. http://www.zurich.ibm.com/security/enterprise-privacy/epal/, IBM, 2004

[CaPB03] Casassa Mont, M., Pearson, S., Bramhall, P.: Towards Accountable Management of Privacy and Identity Information, ESORICS 2003, 2003

[Ibmt04] IBM Tivoli: IBM Tivoli Storage Manager for Data Retention, 2004

[BJSW02] Bettini, C., Jajodia, S., Sean Wang, X., Wijesekera, D.: Obligation Monitoring in Policy Management, 2002

[DDLS01] Damianou, N., Dulay, N., Lupu, E., Sloman, M.: The Ponder Policy Specification Language, 2001

[HFPS99] Housley, R., Ford, W., Polk, W., Solo, D.: RFC2459: Internet X.509 Public Key Infrastructure Certificate and CRL profile. IETF, 1999

[AKSX02] Agrawal, R., Kiernan, J., Srikant, R., Xu, Y.: Hippocratic Databases. IBM Almaden Research Center, 2002

[Ande96] Anderson, R. J.: The Eternity Service. Proc. PRAGO-CRYPT 96, CTU Publishing House, Prague, 1996

[EFL+98] Ellison, R.J., Fisher, D.A., Linger, R.C., Lipson, H.F., Longstaff, T.A., Mead, N.R.: Survivability: Protecting your Critical Systems. Proceeding of the International Conference of Requirements Engineering, 1998

[KBC+00] Kubiatowicz, J., Bibdel, D., Chen, Y., Czerwinski, S., Eaton, P., Geels D., Gummadi, R., Rhea, D., Weatherspoon, H. , Weimer, W., Wells, C., Zao, B.: OceanStore: An Architecture for Global Scale Persistent Storage. University of California, Berkeley, ASPLOS 2000, 2000

[Neum99] Neumann, P.G.: Practical Architectures for Survivable Systems and Networks. SRI International, Army Research Lab, 1999

[WBS+00] Wylie, J.J., Bigrigg, M. W., Strunk, J. D., Ganger, G. R., Kiliccote, H., Khosia, P.K.: Survivable Information Storage Systems. IEEE Computer, 2000

[Casa04] Casassa Mont, M: Dealing with Privacy Obligations: Important Aspects and Technical Approaches. To appear in proceeding of the 1st International Conference TrustBus 2004, Springer Verlag, LNCS, 2004