Scenarios for Privacy Rights Management using Digital Rights Management

Korba, Larry; Song, Ronggong; Yee, George; Chen, Y.-C.

National Research Council Canada
Conseil national de recherches Canada

Institute for Information Technology
Institut de technologie de l'information

NRC · CNRC

Scenarios for Privacy Rights Management using Digital Rights Management *

Korba, L., Song, R., Yee, G., and Chen, Y-C.
May 2005

* published in the Proceedings of the 2005 Resource Management Association International Conference (IRMA 2005), San Diego, CA, USA. May 15-18, 2005. NRC 47428.

Canada

Scenarios for Privacy Rights Management Using Digital Rights Management[1]

Larry Korba, Ronggong Song, George Yee, Bomy Chen

Institute for Information Technology, National Research Council of Canada
1200 Montreal Road, Ottawa, Ontario K1A 0R6
(613) 998-3967, FAX (613) 952-7151, Larry.Korba@nrc-cnrc.gc.ca

ABSTRACT

With the growing spate of privacy laws worldwide, managing privacy has become very important. However, even in countries with well-established and understood privacy laws, there are currently no established technological solutions that meet the challenging requirements expressed by privacy regulations. Variants of XML have been created or extended in an attempt to express privacy rights. The question remains: how can a citizen's privacy rights be managed or enforced? This paper describes extensions to a privacy architecture that employs digital rights management to manage individual data privacy. Several scenarios related to the management of personally identifiable information are described, illustrating how the system operates in support of the requirements expressed in the privacy principles.

1. INTRODUCTION

Organizations find it challenging to comply with existing and emerging privacy laws. Making systems compliant with legal privacy regulations requires a multidisciplinary approach. Information Technology specialists build information systems handling personal information. Information Security specialists develop and maintain the system parts that protect storage and transmission of data. Lawyers and/or privacy officers develop policies that when followed would assure a company or organization is in step with the privacy laws of the lands in which it operates, as well as business requirements. Yet others may inspect written policies and implemented systems to ensure compliance is maintained. While this creates a busy picture for those developing and maintaining an organization's privacy policies, other pressures make this picture more bewildering. For instance, Internet-connected corporations may have clients from different countries, requirements from different organizations may differ and, depending on legislation, different data types must be handled differently.

Ideally information systems would automate fulfillment of at least some requirements expressed in law and policy. However, this is not a simple task. Aside from the complications of dealing with legacy systems that may have functions or data used in different facets of the organization's operations, there are currently no "off-the shelf" solutions that implement the legal, regulatory or company-specified privacy requirements across an enterprise. There have been some developments that are moving toward the automation of privacy compliance, e.g., the development of meta-languages to describe data permissions for usage and Digital Rights Management (DRM) for controlling access to files. Both of these technologies offer some promise for the development of systems for privacy rights management.

In this paper we build upon privacy rights management via DRM by describing scenarios supporting key privacy principles. The work was developed in parallel with our involvement in the European Union (EU) Fifth Framework project "Privacy Incorporated Software Agent" [1]. We therefore base our discussions on Directive 95/46/EC [2], the privacy laws for the EU. The analysis and techniques described here however may be applied to other jurisdictions.

Section 2 briefly describes our work to date in this area. Section 3 provides details of how several key privacy principles would be implemented in a rights management framework. In section 4 we describe some related research supporting this work followed by conclusions in section 5.

2. BACKGROUND WORK: DRM FOR PRM

Korba and Kenny describe an architecture employing rights management and extensions to XML [3] and ODRL [4] to manage privacy rights. The system has four entities: Data Subject (person who is individual of the personal data), Personal Data (or Personally Identifiable Information (PII)), Data Controller (person, agency, public authority or other body which alone or with others specifies the purposes and means of processing personal data), and Data Processor (person, agency, public authority or other body, which processes personal data in contract with the controller).

In the EU, application of the Data Directive (privacy laws) varies within member states. However, a set of nine privacy principles express the intent of the Data Directive [1], and simplifies understanding of compliance. They are:

1. Reporting the processing	All non-exempt processing must be reported in advance to the national Data Protection Authority.
2. Transparent processing	The data subject must be able to see who is processing his/her PII and for what purpose. The data controller must keep track of all processing it and data processors perform and must make it available to the user.
3. Finality & Purpose Limitation	PII may only be collected for specific, explicit, legitimate purposes and not further processed in a way that is incompatible with those purposes.
4. Lawful basis for data processing	PII processing must be based on what is legally specified for the type of data involved, which varies depending on the type of PII.
5. Data quality	PII must be as correct and as accurate as possible. The data controller must allow the citizen to examine and modify all data attributable to that person.
6. Rights	The data subject has the right to improve his/her PII as well as the right to object regarding the execution of these principles by the data controller.
7. Data traffic outside EU	Exchange of PII to a country outside the EU is permitted only if that country offers adequate protection. The Data Controller assures appropriate measures are taken in that locality if possible.
8. Data Processor processing	If data processing is outsourced to processor, controllability must be arranged.
9. Security	Measures are taken to assure secure handling of PII.

Of course the picture for Data Processors, Controllers and Subjects with respect to handling of personal data is far more involved and complex than what is described above. Often Data Subjects do not know which Controllers have what data, and whether it is accurate. Data Controllers and Processors may lose track of the data entrusted to them. This paper further develops privacy rights management through particular data management cases intended to illustrate legal compliance while at the same time simplifying implementation requirements.

2.1. Privacy Rights Management (PRM) Description

Digital rights management (DRM) was conceived to facilitate controlled distribution of digital content and to combat breaches of copyright law. Considerable resources have been expended developing security technologies for content locking and metering, payment, tracking and record keeping. While in DRM these technologies are intended to protect and enforce the copyright of content owners, PRM leverages these technologies for the benefit of the data subject in the protection of their personal data.

The entities involved in DRM include: Digital Content, Digital Content Owners, Distributors and Users/Customers. For PRM, the entities include: Personal Data, Data Subject, Data Controller and Data Processors. To ease adaptation of a DRM system as a privacy rights management system, there is a correspondence between each of their respected entities. Personal Data within PRM is treated as Digital Content within DRM, the Data Subjects in PRM are treated similarly to Content Owners within DRM, the Data Controller has similar functions as the Distributor in DRM, while Data Processors in PRM are similar to Users/Customers within DRM. Further detailed analysis of the development of PRM based upon DRM may be found in [3] and [4].

3. PRIVACY RIGHTS MANAGEMENT IN OPERATION

Within a PRM system, servers handle the functions of the Data Controllers and Data Processors. In order to perform those functions, the Data Controller and Processor servers must maintain and use different data sets. Below we describe the Controller and Processor records and transaction logs required for PRM operation. These descriptions will facilitate understanding of the operational scenarios described section 3.1.

Processor/Controller Related Records

Processors and Controllers maintain 3 key record types: processing agreements, audit information and PII tracking data. They are:

Processing Agreements: These are electronic documents containing arrangement details between the controller and processors including: types of data the processor may accept, limits to the processing endorsed by the Controller, time limits for PII access, agreements and details for audits (timing, type of data collected), and, time stamps and approval signatures for the agreements.

Audit Information: The Controller performs periodic audits of the processor data handling approaches. Audit results include a list of discrepancies between the data held by the processor as compared to those held by the controller. While detailed results are stored in the transaction log, the audit results for the processor/controller are processed/summarized versions of those raw results for controller or processor use.

PII Data Tracking: The controller keeps track of the PII Data sent to each processor, time of the transfers, and pointers to policies and purposes for processing.

Data Subject Related Records

There are several Data Subject-related records maintained by processors and controllers. These include:

PII Data: Personal data entrusted to the controller by the data subject.

Contact Information: Contact information for the PII owner (email address, home address, cross-referenced to PII Data, and policy and purpose for data use).

Audit Information: Processed audit results pertaining to discrepancies in information regarding PII are stored here for review by the data subject.

Agreed-upon policies and purposes: All privacy policies negotiated between the Controller and/or all Processors are stored along with a reference to the affected PII.

Transaction Logs

In order to keep track of all activities by Controllers, Processors and Data Subjects within PRM, the following transaction logs are maintained:

Audit Results: Detailed results from automated periodic, or external audits of the processes used by processor and controller to assure PII is consistent and used only for the purposes and policies specified.

Transfers of PII: Occurrences of transfers of PII. (timing, sender, receiver, and reference to PII involved)

Processing of PII: All Processors record time and duration of PII processing, as well as the policies exercised.

Policy Negotiation/Settlement: Time of occurrence of privacy policy negotiation, with reference to the data subject, processor, and/or controller involved.

Data Subject Interactions: Records are kept of all interactions between data subject and Controller/Processors..

Processor/Controller Interactions: Timing and references details for processor/controller interactions.

3.1 PRM Operational Scenarios

This subsection details PRM in operation by describing scenarios intended to meet several key requirements of key privacy principles. The scenarios include:

- Data Subject enrollment.
- Periodic PII Data audit.
- Data Subject Request for PII data update.

The scenarios are outlined using a description of data flows between the Data Subject, Controller and Processor within the PRM System. Assuring lawful basis of processing is challenging to implement in technology. In this case, approaches that offer potential for solutions in this area are described.

3.1.1 Data Subject Enrollment

Data subject enrollment involves a data subject coming to agreement with a data controller on the PII to be shared, as well as the privacy policy for dealing with the PII and the purpose for which the data may be used or processed. Figure 1 illustrates the data flow between the Data Subject, Data Controller, and two Data Processors.

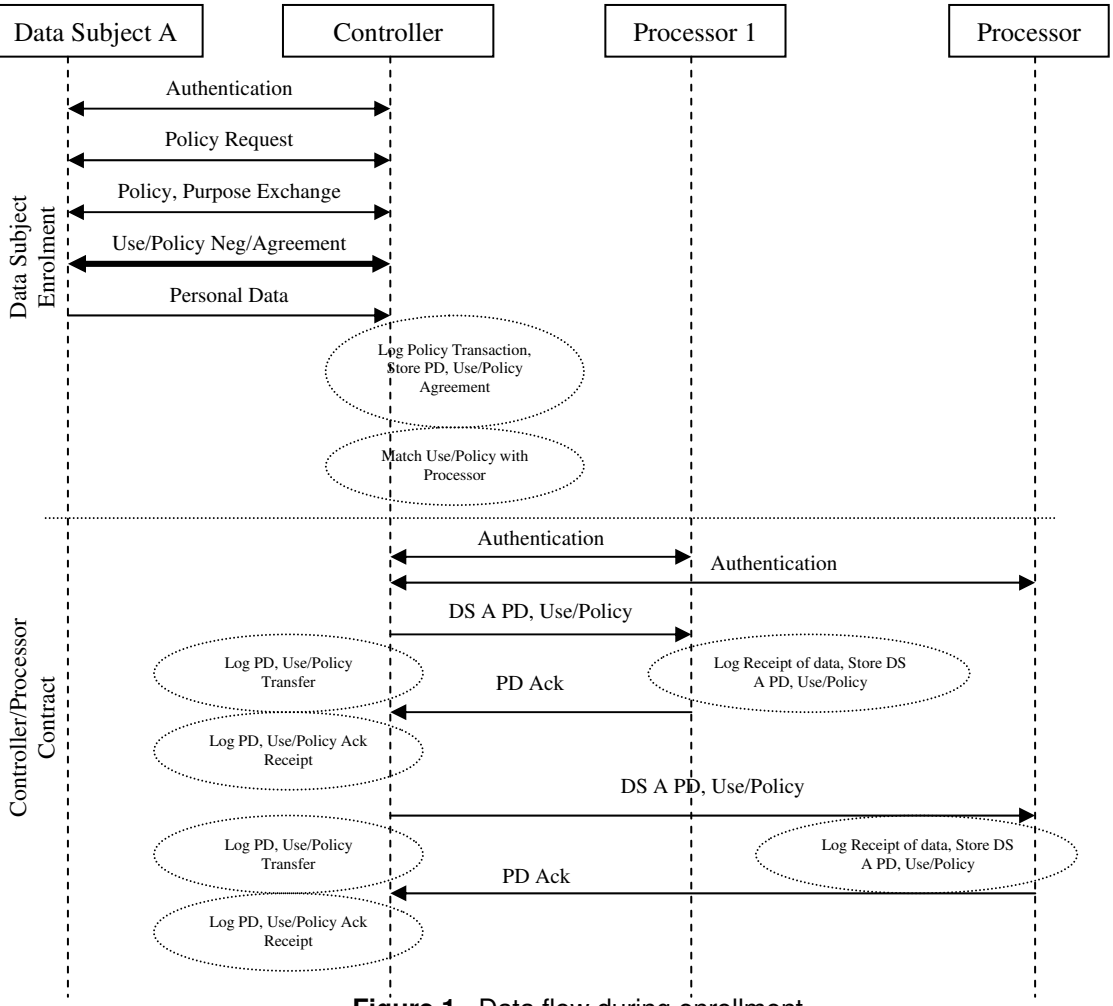

Figure 1. Data flow during enrollment.

The process starts with the Data Subject authenticating herself with the Data Controller. For this and all further exchanges, the Data Subject and Controller set up a secure communication channel between each other. The Controller exchanges a policy and purpose statement regarding the use of any personal data submitted by the Data Subject to the Controller. The Data Subject may negotiate with the Controller for a policy and purpose as described in [5], [6]. When the Data Subject comes to an agreement with the controller on the personal data to be exchanged, as well as the policy and purpose for which the data is being gathered, the data subject provides the data.

The Controller holds the personal data, exchanging it and the use and policy information with the processors that request the data. A number of log entries are made at various times during all of the exchanges. Figure 1 illustrates the various stages for enrollment in detail.

3.1.2 Periodic PII Data Audit

Overseeing PII distributed amongst the Data Controller and Data Processors requires considerable effort and care on the part of the Data Controller. The Controller may have to deal with requests from Data Subjects or more detailed investigations conducted from data protection authorities. Such requests will concern the quality of the data under purvey of

the Data Controller. Operating in a reactive mode to these investigations would be less desirable than a proactive approach wherein the Data Controller assesses the quality of PII under its purvey on a periodic, audit basis as illustrated in Figure 2.

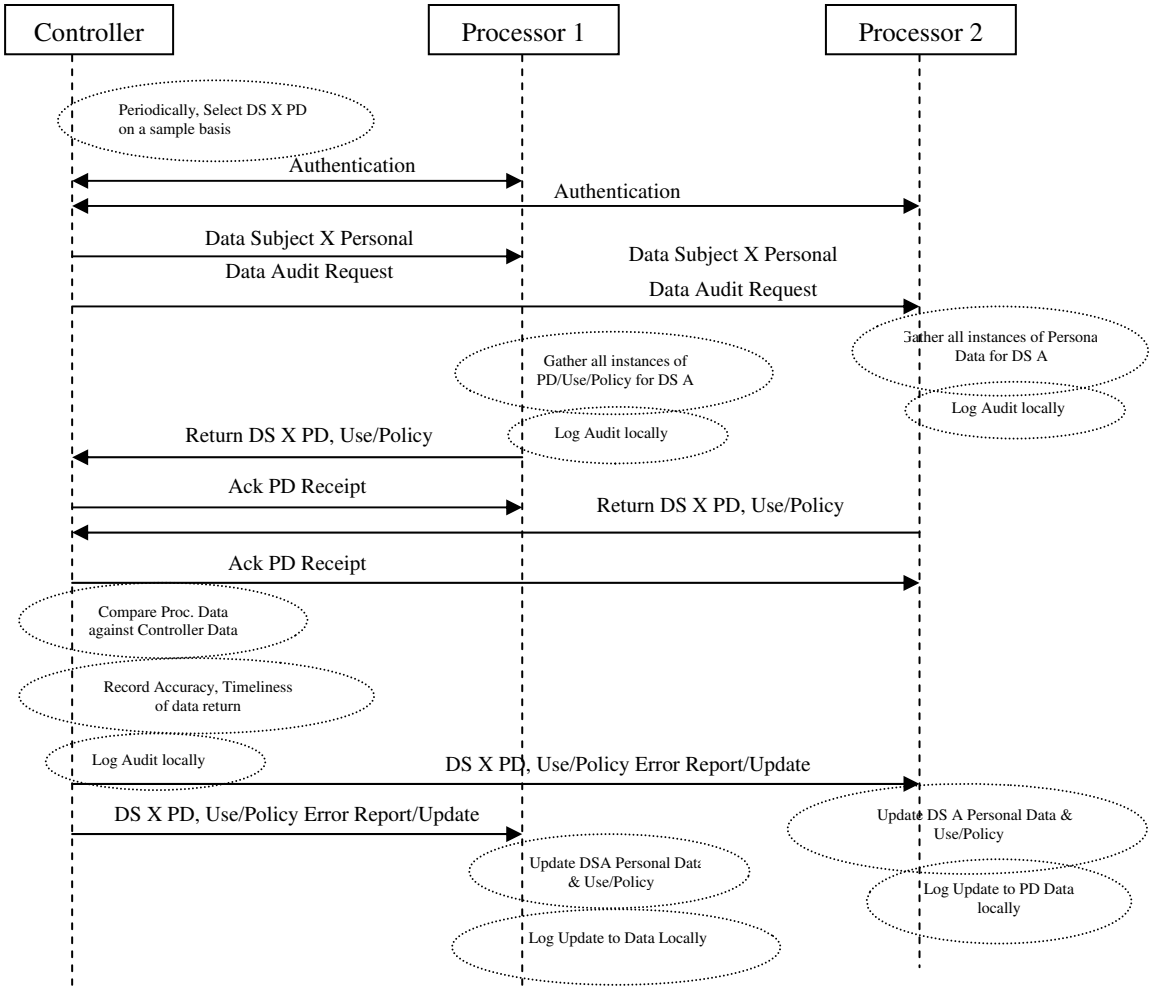

Figure 2. Data flow during periodic Personal Data Audit.

The frequency of the audit depends on the amount of personal data held by the Controller and Processors and the desired level of quality. The Controller periodically selects PII from different data subjects (Data Subject X in Figure 2), polls all processors, requesting them to return PII, policies, and purposes. The processors return the data (if any) they have for the selected Data Subject. From its records, the Controller determines whether or not the Processor should have the data, and tests the congruity of the PII, policies, and purposes, by comparing returned data with its own records.

3.1.3 Personal Data Update by Data Subject

The data quality of PII held by the Data Controller must be maintained. The Controller may receive a request from a subject to check its relevant PII. Figure 3 implements this process. The Controller compares the data it distributed to the Processors against the original data received from the Data Subject. Differences in PII or Policies and Purpose are recorded and reported to the Data Subject. Changes in PII requested by the Data Subject are recorded at the Data Controller and sent to Data Processors that currently have the agreements with the Controller.

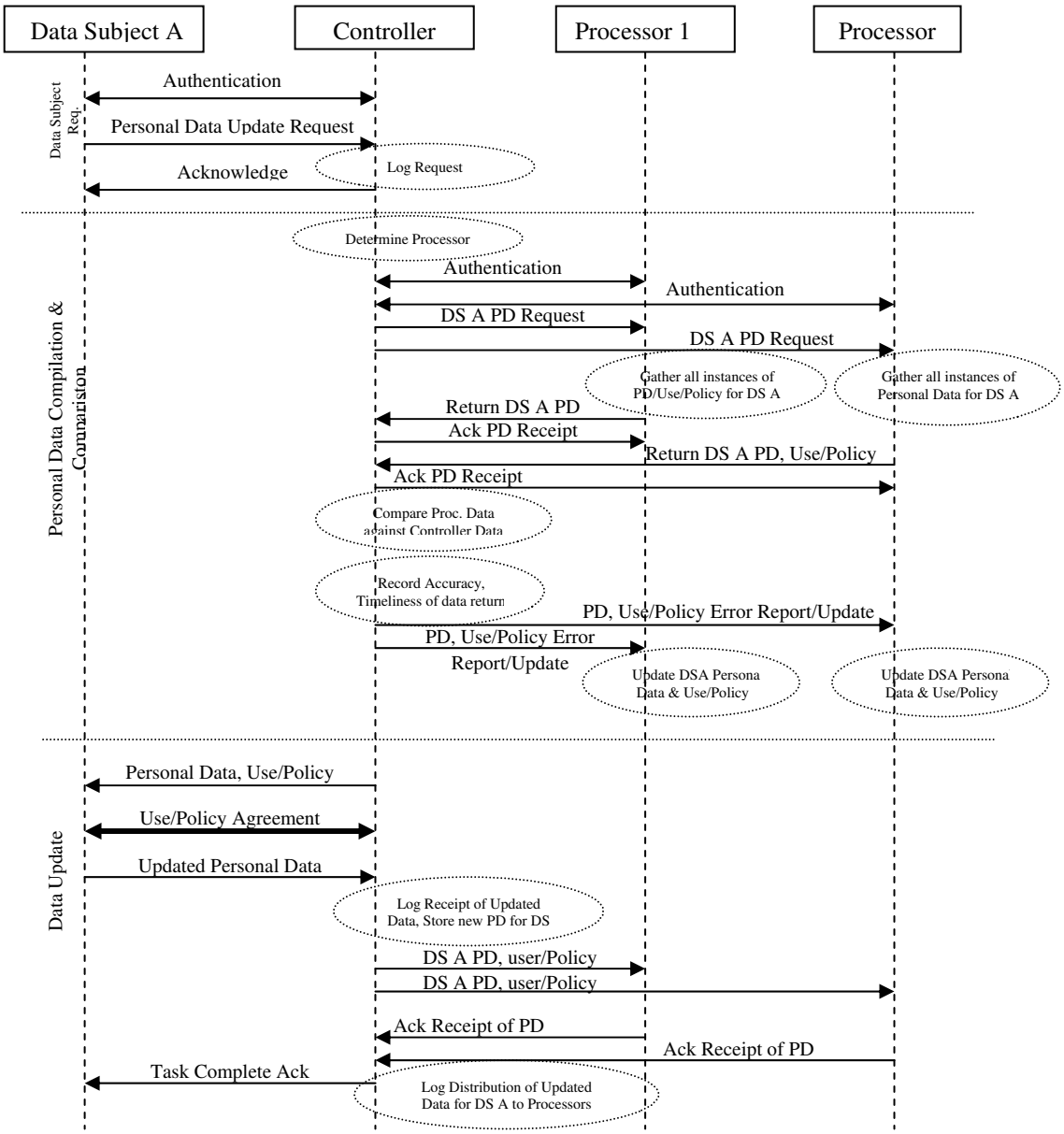

Figure 3. Diagram showing the key interactions between Data Subject. Controller and two Processors during a user request for a change in Personal Data.

3.1.4 Assuring Lawful Basis for Data Processing

For a Data Controller to maintain lawful basis for data processing, it must "control" processing performed by Data Processors. It is very difficult to assure that a Data Processor only processes any PII data for specified purposes. Once a Data Processor has the subject data in the clear, any sort of processing is possible. However, some approaches to limiting the processing may be taken by the Data Controller:

- Audited Contracts. The Data Processor enters into a contract with the Data Controller limiting processing. Under the contract, the processor must maintain records of processing. The Data Controller may audit the records of the processors. The Data Controller may attempt to include the Data Processor in any liability for incorrect processing.
- Metered Access. The Data Controller meters access to the personal data in the same fashion as digital media is metered in a DRM system. This provides the Data Controller with records for all accesses. Unfortunately, this approach is cumbersome, requiring processing/network overhead.

- Certified Third Party Processing. A certified third party would be responsible for all processing; Data Processors and the Data Controller would contract with a certified third party Processor (e.g. data protection authority) only for the processing permitted by law.
- Binding the processing with the PII. It may be possible to bind allowed processing to the PII involved, such that the Data Processor would only be able to process the data in agreed upon ways. Research in the area of security for computation in hostile environments [7] may offer some near-term solutions, however current work [8] indicates that integration of these approaches for large-scale data mining functions is not yet feasible.

Compliance with laws and/or regulations would be the outcome of assuring lawful basis. Currently lawful basis is maintained by careful analysis by Data Controllers and data protection authorities of the privacy impact regarding type of data collected, storage and processing means, and processing types involved. This is a costly process. Interestingly, regulatory compliance is a high priority for corporations of all types in the face of new laws governing the maintenance and disclosure of financial records (e.g. Sarbanes-Oxley, Health Insurance Portability and Accountability Act). The Semantic Web and the legal ontology approach for organizing knowledge [9] offer tremendous possibilities for application in the legal area. In fact, research has been underway for some time to develop a legal ontological approach towards building legal understanding [10]. Eventually, legal ontology may be used to help build legally-compliant applications.

4. RELATED WORK

Karjoth et al. have described an approach for outlining authorization details and options for the use of personal data within an enterprise [11]. The resulting Enterprise Privacy Architecture Language (EPAL) for expressing privacy requirements or regulations [12]. The privacy model and EPAL are well suited to implement the scenarios and data flows described in this paper, due to the considerable flexibility and granularity offered by EPAL. Moreover, the scenario described here articulate, how an enterprise privacy architecture would support several key privacy principles.

Interestingly, IBM and the Information Privacy Commission of Ontario have developed an EPAL representation of the Freedom of Information and Protection of Privacy Act of Ontario [14]. This work is exemplary of some current work creating and using electronic representations of laws. However, while it is commendable to develop an electronic expression of one specific law as a test of the suitability of EPAL for the task, current EPAL and XML tools allow development of electronic expressions of laws or regulations only by computer scientists (XML expertise required). As well, the approach does not effectively build upon the considerable research accomplished and tools developed in legal ontology and the semantic web [9][10].

More recently, Gunter et al. have described applying DRM for privacy management in the context of location-based services [13]. This work develops access control approaches based upon early work in security architectures and applies them in a digital rights management context. In contrast, this paper takes these ideas much further by describing data flows between different entities to provide privacy principle-aware functionality, beyond access control approach.

5. DISCUSSION AND CONCLUSIONS

In earlier works we described the suitability of digital rights management architecture for privacy rights management [3], [4]. Practical scenarios in this paper show how this privacy rights management architecture facilitates enforcement of several key privacy principles of the Data Directive. The Data Subject enrollment scenario deals with the following principles: finality & purpose limitation, transparent processing (through the formalization of Data Subject preferences for processing), and, data processor processing (by providing policies for PII handling). Periodic PII Data Audit supports: Transparent Processing, finality & purpose limitation, data quality, rights, and data processor processing. PII update by the Data Subject supports: rights, data processor processing, and transparent processing. The principle of security is supported throughout via security technology embedded within the use of DRM security to protect PII, and by the use of secure messaging, data channels and data logs. A particularly difficult principle to enforce is “assuring lawful basis for processing”. We describe several developments that offer promise for technical solutions for this requirement. We also propose a model of application development based upon legal ontology so as to develop applications that are legally compliant. The next steps in this work include the development of further scenarios and the integration of several of them with other privacy technologies for privacy policy creation and management, lightweight, yet flexible authentication and authorization techniques, trustable human computer interaction and network privacy.

6. ACKNOWLEDGEMENTS

The authors acknowledge the support of the National Research Council of Canada, and the Communications Security Establishment of Canada for their support in this work.

[1] NRC Paper Number: 47428

7. REFERENCES

[1] Privacy Incorporated Software Agent (PISA) 2001-2004 EU Fifth Framework project at: http://www.pet-pisa.nl/
[2] Official Journal L 281, 23/11/1995, 0031 - 0050
[3] Kenny, S., Korba, L. Adapting Digital Rights Management to Privacy Rights Management, Computers & Security, Vol. 21, No. 7, November 2002, 648-664.
[4] Korba, L. Kenny, S. Towards Meeting the Privacy Challenge: Adapting DRM, DRM 2002, Washington, D.C., November, 2002.
[5] Korba, L. Privacy in Distributed Electronic Commerce, Proc. 35th Hawaii International Conference on System Science (HICSS), Hawaii, January 7-11, 2002.
[6] Yee, G., Korba, L. Bi-Lateral E-Services Negotiation Under Uncertainty, The 2003 International Symposium on Applications and the Internet, January 27-31, 2003, Orlando, Florida.
[7] Yao, A.C. Protocols for secure computations, Proceedings for 23rd IEEE Symposium on Foundations of Computer Sciences 160-164. IEEE Computer Society Press, 1982.
[8] U. Feige, J. Kilian and Moni Naor A Minimal Model for Secure Computation, Proceedings 26th Annual ACM Symposium on Theory of Computing, Montreal, Canada, 1994, pp. 554-563.
[9] W3C Web-Ontology (WebOnt) Working Group, at: http://www.w3c.org/2001/sw/webont
[10] Gangemi, A., Prisco, A., Sagri, M.-T., Steve, G., Tiscorania, D., Some ontological tools to support legal regulatory compliance, with a case study, at: http://www.loa-cnr.it/Papers/WORM-CORE.pdf
[11] G. Karjoth and M. Schunter. A Privacy Policy Model for Enterprises. In *15th IEEE Computer Security Foundations Workshop*. IEEE Computer Society Press, 2002.
[12] Enterprise Privacy Architecture Language (EPAL), available at: http://www.zurich.ibm.com/security/enterprise-privacy/epal/
[13] Gunter, K. May, M., Stubblebine, S. A Formal System and its Application to Location Based Services, Workshop on Privacy Enhancing Technologies (PET2004), May 26-28, 2004, Toronto, Ontario.
[14] Adler, S. IBM Enterprise Privacy Solutions, 12th CACR Information Security Workshop & 4th Annual Privacy and Security Workshop: Privacy and Security: The Next Wave, Nov. 6-7, 2003, Toronto, Ontario,