Privacy Rights Management for Privacy Compliance Systems

Song, Ronggong; Korba, Larry; Yee, George

Publisher's version / Version de l'éditeur:

Proceedings of the 21st IEEE International Conference on Advanced Information Networking and Applications (AINA Workshops Symposia 2007), 2007

Privacy Rights Management for Privacy Compliance Systems

Ronggong Song, Larry Korba, George Yee
Au Institute for Information Technology, National Research Council of Canada
Ronggong.Song, Larry.Korba, George.Yee}@nrc-cnrc.gc.ca

Abstract

The worldwide growth of e-services has brought to the forefront the importance of citizen privacy management. Korba and Kenny proposed a privacy rights management system in order to support the privacy principles derived from EU Data Directive 95/46/EC of the European Parliament and the Council of 24 October 1995. In this paper, we extend their system by proposing a privacy rights management framework for entity modeling and expression. The proposed framework manages and monitors the use of personal information. In addition, it provides interoperable mechanisms to support privacy compliance systems.

1. Introduction

With the growth of e-services worldwide (e.g. e-government, e-health, e-learning, and e-commerce, etc.), managing citizen privacy has become an important issue, especially within western democratic countries. For instance, according to the Directive [1] expressing the protection of European Union Citizens' personal data, the right to privacy is defined as a human right under Article 8 of the 1950 European Convention of Human Rights and Fundamental Freedoms. Legislation and enforcement structures similar to the European model exist in Canada, Australia, Norway, Switzerland, and Hong Kong. In order to provide a commonly accepted technological approach that meets the challenging requirements expressed by privacy regulations, Korba and Kenny [2, 3] proposed a privacy rights management (PRM) system which defines Privacy Rights Management as the management of personal data according to the requirements of the Directive.

In order to model and express the rights information of personal data in PRM and support a variety of privacy compliance systems, we propose a privacy rights management framework (PRMF) in this paper. Although many privacy management languages such as P3P [4], APPEL [5], and EPAL [6] exist, these languages do not satisfy many aspects of privacy legislations. For instance, they do not specify how the collected personal data are stored and what security mechanisms are used for safeguards to protect the data (see "Privacy Principle 9: Security" in Section 2.1, Table 1). Many companies just store the personal data as plain text without any security protection (e.g. encryption). They especially do not monitor and record the processing records of the data so that it can be available to the user to know who processed his personal data, for what purpose (see "Privacy Principle 2: Transparent Processing" in Section 2.1, Table 1), and whether the processing is compliant with the privacy legislation (see Privacy Principle 3 and 4). While some aspects related to information flow for PRM are described by Korba et al. [9], we take these ideas further to develop this framework to create a privacy compliance system.

By investigating the existing technology, we define PRMF as the privacy rights management framework for personal data according to the requirements of the Directive and PRM. PRMF contains three important entities: Policy, Processing, and Assessment, in order to comply with privacy legislation and to provide better protection for personal data. Policy is really an agreement which describes the desired privacy protection controls and is signed by both data subject and data processor. Policy contains permissions for personal data usage and data expiration dates. Processing lists the activity events on the personal data. These events contain information regarding who accessed the data, when the data was accessed, and what operations were performed on it. This provides information to let the data subject review the processing of his personal data through various interfaces or mechanisms of PRM. Assessment lists the privacy compliance evaluation results including whether the personal data had been stored securely (e.g. encrypted) and whether the processing events comply with the privacy policy and privacy legislation. When non-compliant processing events happen, the

PRMF can force the privacy compliance systems to stop the processing or alert the data processor. The PRMF provides effective features to comply with the privacy principles of the Directive (EU), the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) [7] and the Canadian Standards Association Model Code for the Protection of Personal Information [8]. We are developing a new privacy compliance system to support PRMF since existing privacy compliance systems do not provide all of the required features.

The rest of this paper is organized as follows. Section 2 briefly describes background research on the Directive and PRM. Section 3 presents our proposed Privacy Rights Management Framework, including models oriented towards the privacy principles in the Directive and the PRM system. Section 4 discusses implementations. Section 5 gives our conclusions.

2. Background

2.1. Privacy principles in the EU

In Europe, the Directive (privacy laws) specifies the protection of rights of data subjects as well as the requirements and responsibilities required of data controllers and their associated data processors [1]. The approach expressed in the Directive is described by a set of nine privacy principles which simplify the understanding of compliance for the Directive. These privacy principles are shown in Table 1.

Table 1. European Union privacy principles [2, 3]

Principle	Description
1. Reporting 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 personal data and for what purpose. The data controller must keep track of all processing it performs and the data processors and must make it available to the user.
3.Finality & purpose limitation	Personal data 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	Personal data processing must be based on what is legally specified for the type of data involved, which varies depending on the type of personal data.
5. Data Quality	Personal data 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 or her data as well as the right to raise certain objections regarding the execution of these principles by the data controller.
7. Data traffic outside EU	Exchange of personal data 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 from data controller to processor, controllability must be arranged.
9. Security	Measures are taken to assure secure processing of personal data.

2.2. Privacy rights management (PRM)

In order to meet the privacy requirements shown in Table 1, Korba and Kenny proposed a privacy rights management system by adapting a digital rights management system. Within the EU context, there are 4 entities for PRM: Personal Data, Data Subject, Data Controller, and Data Processor. Personal Data is the Information that can be linked with a data subject. Some data may be more sensitive than others. The Data Subject is the owner of the personal data. The Data Processor is an organization or individual that processes personal data according to the policies agreed upon with the data subjects. The Data Controller acts as the enforcer of usage requirements for personal data. It manages the collection, storage, and processing of personal data from the data subject. Figure 1 depicts a simplified version of this privacy rights management system.

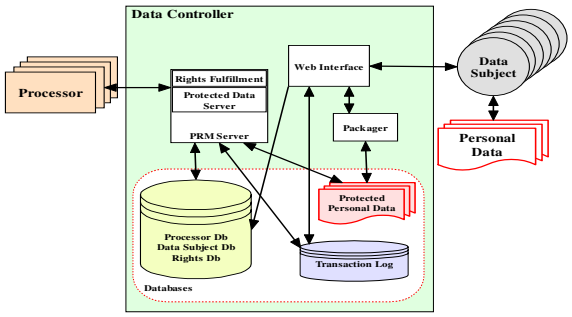

Figure 1. A simplified privacy rights management system

In Figure 1, the Data Controller lies between the Data Subject and the Processor so that it can fulfill its role as the enforcer of personal data usage requirements. The Transaction Log within the Data Controller provides for compliance assessment and accountability.

3. Privacy rights management framework

Our proposed Privacy Rights Management Framework is designed to comply with the privacy principles of the Directive (EU) and PIPEDA (Canada) [7] and offer efficient management for personal data protection through privacy policy agreement, monitoring of personal data processing events, and privacy compliance assessment.

The PRMF consists of three main entities: Policy, Processing, and Assessment. Each main entity contains several other entities. Figure 2 depicts PRMF and the relationships between the entities.

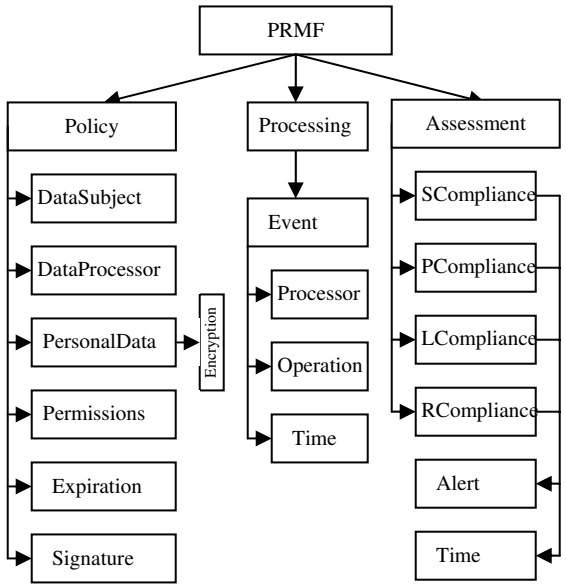

Figure 2. Privacy rights management framework

In the PRMF, the Policy entity expresses the data subject, data processor, personal data, and detailed permissions to limit personal data usage. In order to achieve higher security protection, this policy expression may require digital signatures from both the data subject and data processor. Some sensitive personal information such as SIN number, Credit Card account, and others may require encryption protection to prevent private data leakage. The Processing entity expresses the processing events on the personal data, including the processor, operations performed, and time of the activity. The Assessment entity expresses the privacy compliance evaluation results, including the personal data security compliance (SCompliance) (e.g. evaluate whether the sensitive data are protected properly, whether they have potential for outside leakage or have already leaked out), policy compliance (PCompliance), which evaluates whether the processing of personal data complies with the privacy policy for the organization, legal compliance (LCompliance), which evaluates whether both the privacy policy and processing comply with the privacy principles, and regulatory compliance (RCompliance), which for certain industry sectors, evaluates whether the processing complies with the sector's privacy regulations. (Note that separation into four different assessment entities allows a more focused analysis for the purpose of privacy impact assessment.) Alerts which record the personal data processing events that are non-compliant and their time of occurrence are issued for each non-complying entity. Detailed information about the PRMF entities are described in the following sections.

3.1. PRMF policy model

The PRMF privacy policy model expresses a special privacy agreement between the data subject and the data processor for use of the personal data. This model consists of the Policy branch in Figure 2. The Policy entity is made up of seven other entities.

- DataSubject – usually the owner of personal data, who signs the policy and authorizes certain permissions to the data processor for limiting his personal data usage;
- DataProcessor – the organization (e.g. government, corporation, etc.) or individual who signs the policy and receives certain permissions from the data subject for use of the personal data;
- PersonalData – the personal information of the data subject, which can be categorized as identification information, contact information, financial data, medical data, and others;
- Permissions – the authority to use, transfer, and store the personal data, which is negotiated and agreed between the data subject and the data processor;
- Expiration – the expiration date of the privacy policy that is encapsulated by Policy;
- Signature – the information related to a signature including hash algorithm, hash value, signature algorithm, public key information, and signature value, which provides non-repudiation protection for the privacy policy;
- Encryption – the information related to an encryption including encryption algorithm, key information, and encrypted cipher text. This provides confidentiality protection for the personal data.

The Policy entity provides a set of particular permissions over the personal data, negotiated between

the data subject and data processor to limit the usage of personal data. The encryption and signature offer good security protection for both the personal data and the privacy policy.

3.1.1. PRMF personal data model. The PRMF personal data model expresses the personal data of the data subject according to different categories of personal information. The personal data entity is an aggregation of many other entities based on their categories.

- Identification – the information to identify the data subject such as driver license, health card, social insurance number, birthday, fingerprint, and certificate;
- Contact – the contact information of the data subject like address, telephone number, cell phone number, fax number, and e-mail address;
- Financial – the financial information of the data subject like bank account, credit card, investment, property, and insurance;
- Other categories related to the data subject such as medical data, family information, daily activities, business information, career, etc.

The above categorization also shows the different levels of importance assigned to personal data; for instance, a person usually thinks of his identification, contact, financial, and medical data as being more important than other data. These sensitive personal data may require extra security protection, as provided by the Encryption entity, described in the policy model.

In addition, it may be impractical to store all detailed personal data in the PersonalData entity, especially when the personal data is very large as often is the case for medical data. In this situation, the Personal Data Model can use the DataLocator entity to locate the stored personal data.

- DataLocator – the link information to locate the personal data storage, which could be a URL, directory, or path.

3.1.2. PRMF permissions model. The PRMF permissions model expresses the authorizations for personal data usage under the privacy policy. It authorizes certain rights to allow the data processor to process personal data. The permissions entity is an aggregation of four other entities and their related entities.

- DataSpecifier – the link information to locate which part of personal data requires the permission, e.g. Identification\SIN, Financial\CreditCard;
- Usage – defines the usage authorization part of permission. It contains the following four entities:
  - ❖Purpose – defines a special purpose for using the personal data, e.g. payment;
  - ❖Edit – describes whether or not to authorize editing rights to the data processor for personal data processing;
  - ❖Print – describes whether or not to authorize printing rights to the data processor for personal data processing;
  - ❖Time – defines a time limit or a special period (e.g. once) for personal data processing.
- Transfer – defines the transfer authorization part of permission. It contains the following entities:
  - ❖Processor – defines the destination for the transfer;
  - ❖Purpose – describes the purpose for transferring the personal data, e.g. payment transaction;
  - ❖Time – defines a time limit or a special period for the transfer of personal data.
- Storage – defines the storage authorization part of permission. It contains the following entities:
  - ❖Backup – describes whether or not to authorize backup rights to the data processor for the personal data storage;
  - ❖SecureBackup – describes whether or not to authorize a secure backup for the personal data storage;
  - ❖Time – defines a time limit or a special period for the personal data storage.

The Permissions model provides the detailed authorizations under the privacy policy to limit the personal data usage and processing. It defines who has rights to process the data and for what purpose, and so on.

3.1.3. PRMF encryption model. The PRMF encryption model is important for personal data protection. It expresses the necessary information related to encryption to allow encryption to be straightforward. The encryption entity is an aggregation of three other entities.

- EncryptionMethod – specifies the encryption algorithm used in the Encryption entity, e.g. Triple-DES, AES;
- KeyInfo – specifies the session key information used for the encryption;
- CipherValue – contains the encrypted cipher text by the above encryption algorithm and the session key. It will be stored as indicated by DataLocator if the ciphertext is very large.

The encryption entity provides confidentiality protection for sensitive personal data in PRMF such as identification, financial, and medical data.

3.1.4. PRMF signature model. The PRMF Signature Model expresses the necessary information related to a signature. The signature entity is an aggregation of five other entities.

- DigestMethod – specifies the hash algorithm used in the signature entity, e.g. SHA-1, SHA-256;
- DigestValue – contains the hashing result with the hash algorithm;
- SignatureMethod – specifies the signature algorithm used in the signature entity, e.g. RSA;
- KeyInfo – contains the public key certificate used for the signature;
- SignatureValue – contains the signature result with the private key and the above signature algorithm.

Since both the data subject and the data processor sign the privacy policy using the signature entity, there is non-repudiation protection for the privacy policy agreement so that the two parties cannot deny this agreement when a privacy policy non-compliance event happens later.

3.2. PRMF processing model

The PRMF Processing Model expresses the personal data processing events for tracking the personal data processing. This model consists of the Processing branch in Figure 2. The processing Event entity is an aggregation of three other entities.

- Processor – the organization or individual who processed the personal data for this processing event;
- Operation – the activity that the data processor performed during this processing event, e.g. read, write, modify, delete, copy, print, e-mail;
- Time – the time of the data processor operation.

The processing Event entity provides the detailed personal data processing records to let the data subject track his personal data usage and supports the privacy compliance system in its assessment of whether the processing complies with the privacy policy and privacy principles. Each event corresponds to one instance each of Processor, Operation, and Time.

3.3. PRMF assessment model

The PRMF Assessment Model expresses the privacy compliance evaluation results for the personal data processing in relation to the privacy policy. This model consists of the Assessment branch in Figure 2. The Assessment entity is an aggregation of five entities.

- SCompliance – the privacy compliance evaluation on the personal data security protection, e.g. encrypted, non-encrypted;
- PCompliance – the privacy compliance evaluation on the personal data processing based on the privacy policy, e.g. non-compliance on the personal data storage when the privacy policy shows SecureBackup but the SCompliance value on security for data storage is “non-encrypted”;
- LCompliance – the privacy compliance evaluation on the privacy policy and personal data processing related to privacy legislation, e.g. non-compliance on the privacy policy when the privacy policy shows when according to law, the processor is responsible;
- RCompliance – This pertains to certain industry sectors where there are regulatory requirements for privacy compliance (e.g. banking, health care);
- Alert – the alert information or remedial action according to the degree of non-compliance associated with privacy assessment events, e.g. ignoring, warning, stopping;
- Time – the detailed time for processing this assessment.

The assessment model provides the privacy compliance evaluation results on the privacy policy and the personal data storage and usage. The evaluation is processed by the privacy compliance assessment module of privacy compliance systems according to the privacy policy, personal data processing events, privacy legislation, and the privacy regulations of certain industry sectors.

4. PRMF practice

To demonstrate PRMF, we developed an agent-based privacy compliance system. The architecture offers efficient management for the personal data protection through the Data Controller Agent, Privacy Compliance Monitoring Agent, Privacy Compliance Assessment Agent, and Privacy Compliance Enforcement Agent. Figure 3 depicts the data controller agent on the data controller’s machine and the privacy monitoring agent, privacy assessment agent, and privacy enforcement agent on the data processor’s machine.

In the system, privacy-related events detection technologies are used to filter the monitored activities for the privacy-related event data collection. The key technologies for this purpose are the private data and event detection patterns. For the prototype, we have implemented some detection patterns related to identity, contact, and financial data such as social insurance number (SIN), credit card number, bank account number, phone number, postal address, e-mail address, keywords, and others. Figure 4 depicts an example of a personal data processing detection report.

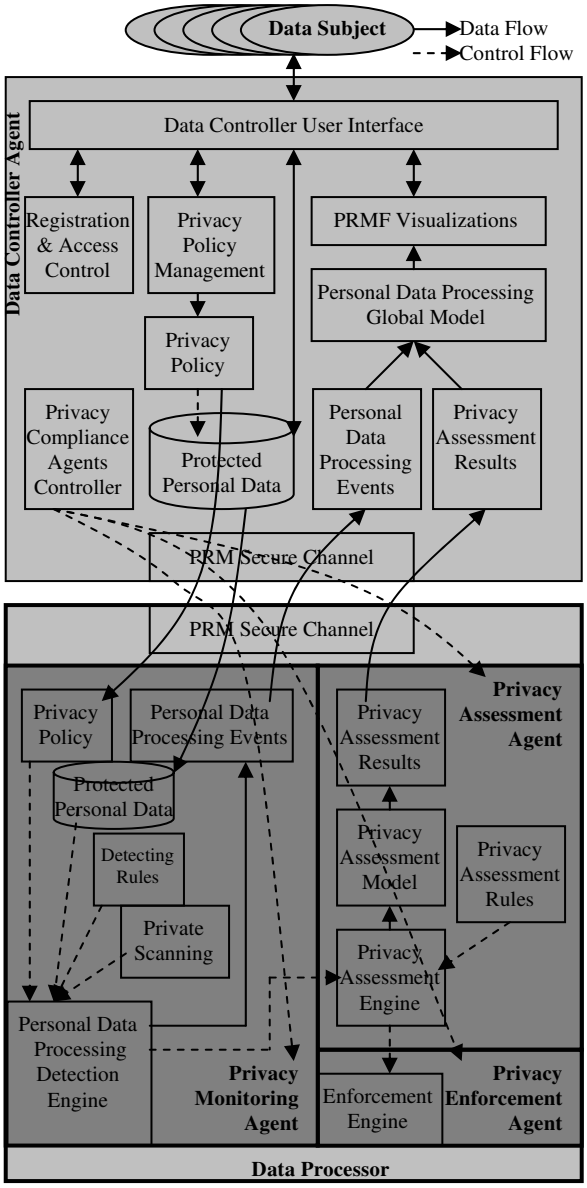

Figure 3. Agent-based privacy compliance system.

Figure 4. Private Data Detection Report

5. Conclusions

In order to provide better protection for personal data, we propose PRMF, a privacy rights management framework which enforces personal data processing compliance with privacy policies related to organizational, legislative, and regulatory needs. In this paper, we have provided a description of this framework and all its different entities. PRMF can satisfy many aspects of privacy legislation, including security, transparent processing, lawful basis, and finality & purpose limitation.

We are developing a new privacy compliance system based on the features and definitions of PRMF.

6. References

[1] EU Directive 95/46/EC. EU Official Journal of the European Communities, No L. 281, 23/11/1995 p/0031--0050.

[2] L. Korba and S. Kenny, Towards Meeting the Privacy Challenge: Adapting DRM, DRM 2002, Washington, D.C., November, 2002.

[3] S. Kenny and L. Korba, Adapting Digital Rights Management to Privacy Rights Management, Journal of Computers and Security, Vol.21, No.7, November, 2002.

[4] L. Cranor, B. Dobbs, S. Egelman, G. Hogben, J. Humphrey, M. Langheinrith, M. Marchiori, M. Presler-Marshall, J. Reagle, M.Schunter, D. A. Stampley, and R. Wenning. The Platform of Privacy Preferences 1.1 (P3P 1.1) Specification. Retrieved June 29, 2006 from http://www.w3.org/TR/2006/WD-P3P11-20060210/.

[5] L. Cranor, M. Langheinrith, and M. Marchiori. A P3P Preference Exchange Language 1.0 (APPEL 1.0). Retrieved June 29, 2006 from http://www.w3.org/TR/P3P-preferences/

[6] P. Ashley, S. Hada, G. Karjoth, C. Powers, and M. Schunter. Enterprise Privacy Authorization Language (EPAL 1.1). M. Schunter (Ed.). Retrieved June 29, 2006 from http://www.zurich.ibm.com/security/enterprise-privacy/epal/Specification/index.html.

[7] Office of Privacy Commissioner of Canada. The Personal Information Protection and Electronic Documents Act. Retrieved June 29, 2006 from http://www.privcom.gc.ca/legislation/index_e.asp.

[8] Canadian Standards Association. Model Code for the Protection of Personal Information. Retrieved June 29, 2006 from http://www.csa.ca/standards/privacy/code/Default.asp?articleID=5286&language=english.

[9] L. Korba, R. Song, G. Yee, and Chen, Y.-C. Scenarios for Privacy Rights Management using Digital Rights Management, Proceedings of the 16th International Information Resources Management Association Conference (IRMA 2005), San Diego, California, USA. May 15-18, 2005. NRC 47428.