International Journal of Multimedia and Ubiquitous Engineering
Vol.9, No.3 (2014), pp.203-212
http://dx.doi.org/10.14257/ijmue.2014.9.3.19

The Sensitive Information Management System for Merger and Acquisition (M&A) Transactions

Kyong-jin Kim* and Seng-phil Hong**

Sungshin Women's University
{kyongjin, philhong}@sungshin.ac.kr
** First author, ** Corresponding author*

Abstract

In M&A transactions, there are many 'data' to be handled to complete any given transaction. There are personal and private data in nature to be transferred and examined during the due diligence process and completing the Representations and Warranties in the final contract. The due diligence sometimes requires "personal data" includes supplier and employee data. In most of the countries, data protection issues have long been neglected in merger and acquisition transactions. However, personal data in many forms can be accessed and may be disclosed even without the knowledge of the information owners. To solve the privacy issues in M&A transactions, we introduce a reliable system in M&A to support access protocol based on privacy policies. Our system helps to securely transfer from the target to the acquirer for any given M&A transaction.

Keywords: *M&A transaction, Private data, Policy management, Privacy protection, Compliance*

1. Introduction

Many M&A activities take place without too much of protection of private information. But business professionals including business lawyers should take into account the impact of privacy laws on business transactions. They need to consider whether any sensitive personal information is being transferred or disclosed. If so, consents by the information owner to such transfers are required. The private information often get accessed during the due diligence process and fulfilling the representations and warranties for the final contract [6, 8].

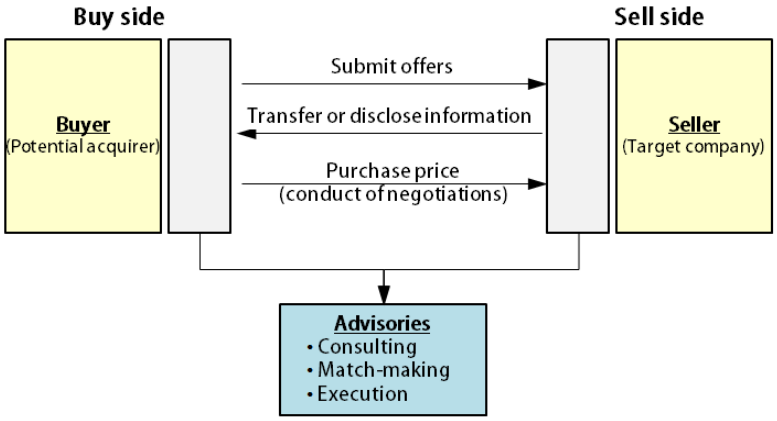


Figure 1. The buying process

ISSN: 1975-0080 IJMUE

In an M&A transaction, the parties are confronted with various disclosure requirements before, during, and after closing. The question of whether certain sensitive private information may be disclosed at a certain point in the transaction may have privacy implications. There should be no collection, use or disclosure, and store of personal information without consent. Technically, consent is to be required for the disclosure of personal information by a target organization to a potential acquirer for due diligence purposes. To avoid private data disclosing risks, the potential purchasers almost always enter into confidentiality agreement. But even with the non-disclosing agreement, there need to be a formal process to make sure the private information is not to be handled carelessly [1, 9].

In the representations, warranties and indemnities, in Purchase and Sales Agreements, sellers may seek to specifically exclude any representations and warranties respecting compliance with privacy laws. But purchasers almost always seek to include the private information [2, 4]. There are two types of personal information the target company has;

- Private information of employees
- Personal information collected, retained, used and disclosed as a part of its ongoing business operations.

There should be some rules [1, 2] in accessing the private information for an M&A process;

1. **Disclose sensitive information only what is necessary for the process;** while it is understandable that the acquiring party seeks to find out as much as it can about the target company so that rational pricing decisions can be made and appropriate documentation can be created, accessing private information beyond necessity may burden the acquirer for compliance issue.
2. **Access only if an as necessary;** when acquirers to remotely access personally identifiable information contained in data bases and data rooms may cause them to comply unnecessary privacy problems.
3. **Privacy and data security due diligence is critical;** careless acquisition of personal data can transfer existing liabilities to the acquiring party. A careful review of the target company's privacy policies and practices is necessary.
4. **Post acquisition data integration is critical;** the management of privacy and data security issues in business transactions does not end with the signing of definitive agreements or even closing the deal. The integration of the privacy and data security practices of two companies is an ongoing process.

In this paper, we are to focus on the private HR data and clients' personal information transferred from the target to the acquirer. Oftentimes, acquirer wants to ensure employee retention after the completion of the transaction to maintain the core competency and productivity of the target company. We present a reliable system to support the privacy policies of an M&A transaction.

2. Problem Statement and Alternatives

2.1. The personal information classification

Personal information includes any factual or subjective information, recorded or not, about an identifiable individual. The information in any form of the followings;

- Corporate confidential information: collected clients' personal data
- HR data of employees: Age, name, ID numbers, income, address, ethnic origin, information of next of kin, academic background, credentials, career history, performance review, and employees' medical record

However, we assume the collected clients' personal data of the target company will not be disclosed during the acquisition process. Disclosing such information is illegal in most jurisdictions. Therefore, we can only focus on the HR data of the target company's employees. HR data can be very important if the target company's corporate performance or productivity depends largely on some of the key personnel. For example, if the target company is an on-line game developer, the main architect of the game is perhaps the most important asset of the company. It will be even more so if the target company is a professional service firm such as law firm, management consulting services, and teaching institutes. The firm's reputation is of course very important, but the detailed information of the professionals of the target firm is critical in considering the corporate value.

2.2. Private information disclosure by types of M&A transaction

There are many different types of M&A transactions, but most common transaction types are either in the form of auction or private deal. For simplicity and generalization, we assume there is only one seller with one target company for any given M&A transaction.

Table 1. Types of M&A transaction

	Auction	Private Deal
Engaging players	Multiple potential buyers at once	One potential buyer at a time
Data accessing method during the due diligence process	Remote access to Data Room Emails, printed copy of documents	Physical access of data, emails, printed copy of document
Access control of data	Difficult to trace the data breach	Relatively secure and easy

As we can see from the above table, accessing the private information in auction process can be more frequent than private M&A deal process.

2.3. How to grant access and what to disclose to whom?

There is a system administrator of the data room who may have full access to the information of course. They also have to follow the access protocol of the private information. The level of information disclosing can be different based on the importance of the personnel of the target company as follow.

Table 2. Information access rights

	Buy side	Sell side	(Buy/Sell) Advisories
Information Creating rights	No	Yes	No
Read and download	Yes (partial download rights)	Yes	Yes (partial download rights)
Use of private information	For the acquisition purpose only upon consent of the information owner or signing the NDA	For the given purpose only with the prior consent of the information owner	For the acquisition purpose only upon consent of the information owner or signing the NDA
Store of the data	No	Yes	No
Destroy or return of the data	Yes	Yes	Yes

Table 3. Information disclosing based on the level of employment

Employee type	Private information	Upon special request
Owner (Majority Shareholder)	Name, DOB, address, income, ethnic origin, academic background, credentials, career history	Information of next of kin, medical record, personal financial information
C-Level executives	Name, DOB, address, income, ethnic origin, academic background, credentials, career history, performance review, medical record	Information of next of kin, personal financial information
Core personnel other than C-level	DOB, income, academic background, credentials, career history, performance review, medical record	Information of next of kin
General employees	DOB, income, academic background, credentials, career history, performance review,	Medical record
Outside directors and/or advisors	DOB, income, academic background, career history	Information of next of kin

3. Sensitive Information Management System

Our proposed SIMS aims to manage the private HR data based on privacy policies in M&A transaction. It could make the privacy policies using the extensible access control markup language (XACML) [5] to specify role-based access control (RBAC) policies, and helps to reasonably disclose to private information of the target company's employees. SIMS consists of four distinct parts: a Policy Loader Mechanism, a Policy Decision Mechanism, a Policy Treatment Mechanism and a Detect Monitoring Mechanism. An overall view of the system is shown in Figure 2.

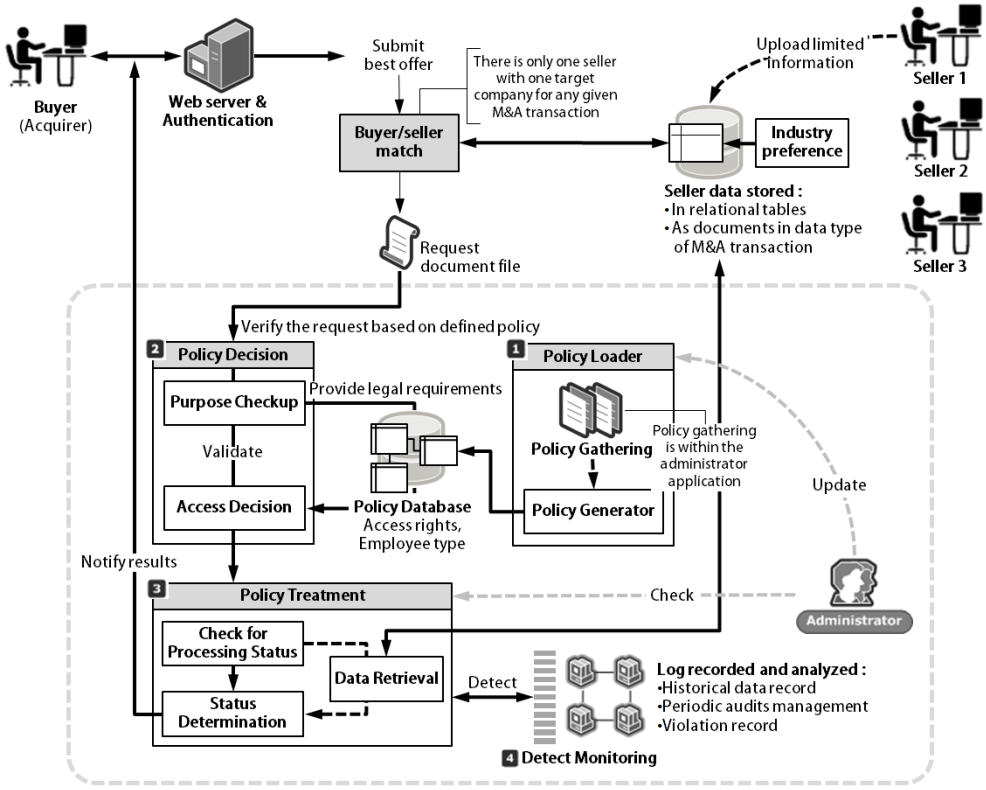


Figure 2. Sensitive information management system

Privacy issues are becoming increasingly important aspects of society, and personal information is generally considered to be private in M&A transactions. In fact, the legal validity surrounding personal information in Korea exists in the Personal Information Protection Act (PIPA) 2011 [7]. The key privacy principles of this law are based on the EU directive and the OECD guidelines, and these are expressed in natural language. Therefore, it is important to represent the formal privacy specification automatically. Our approach uses **1) the Policy Loader Mechanism** to set the privacy policies, which provides the criteria of legal validity and obligations. The mechanism classifies private information of target's company employees by importance, and this specifies to set the type of service according to an M&A process.

In this system, an authentication is a method of identification based on Internet personal identification number (i-PIN) [3]. This authentication method may involve verifying whether a user such as an acquirer is suitable for M&A transactions. We can have an effective check of the request document after an authentication and a match. The request document, which is based on XACML technology, relates to the disclosure of privacy information of the target company, and can be required to access the private information for an M&A process. To support XACML for privacy policies, this mechanism can automatically generated a machine-readable XML format.

2) The Policy Decision Mechanism can automatically analyze the request document with checking their authenticity or suitability. Each purpose classifies the processing of the personal data as one of four phases of the lifecycle (namely from its collection, retention, use and destroy), as shown in Figure 3. The access decision function allows the applicability established by the privacy policy, and then it supports the privacy policies to comply with

security laws including Korea's privacy laws, regulations and OECD guidelines. It is also important to check for one or more conditions. Conditions are defined as an essential requirement such as consents by the information owner that must be met or fulfilled by privacy policies. This mechanism is to check whether the condition is fulfilled, and then determine whether the requested actions should be allowed or denied. The applicable law includes a requirement that the individuals involved must be notified in the case of data processing. For this reason, the mechanism proposed in this paper, the target company's employees have the right to informed consent prior to the processing of their personal information.

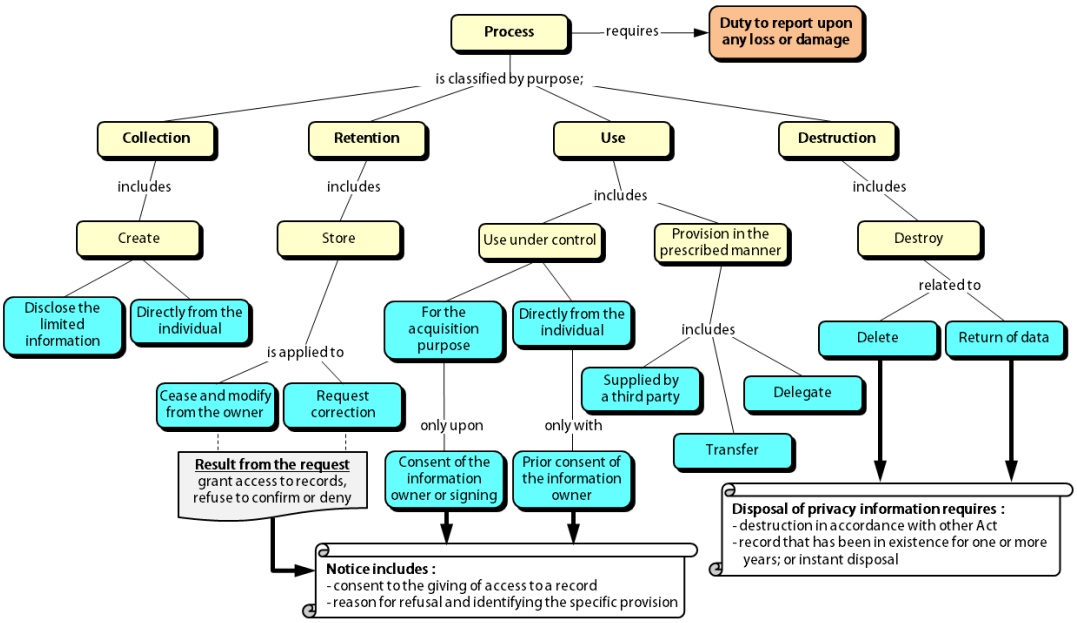


Figure 3. Type of process and relationship

The system administrator should be checked the request document.

3) The Policy Treatment Mechanism may require a system administrator to request advanced approval related to the processing of personal data by an acquirer. It supports to write the record of the approval/reject request according to the 5 Ws and one H. It also helps to provide the verification process by an administrator, and thus reduces the incidence and ensures the accountability. The retrieved information is then provided to the acquirer according to that of the result of processing, and the information owner will be notified about the occurrence of such a decision. The result in this mechanism is built on XACML. This document indicates the status of process and specifies the protection policies. Since it is based on XACML, it can be applied to the target company's privacy policies and practices as well as privacy laws, and then extended to accommodate the unique requirements.

4) The Detect Monitoring Mechanism can record log files. These files are a recording of everything that transferred or disclosed during the acquisition process. To measure the safety of a system administrator, it also records the historical data. In particular, this mechanism has detected suspicious activities, such as attempts to gain unauthorized access or accesses to

large amounts of personal data. The system administrator can restrict unauthorized access to personal data when such events occur. The access also should be limited to specific IP addresses and identifier names. In addition, this will alert the information owner (or majority shareholder) when the system detects suspicious activity. The system administrator must be checked the monitoring that can be used to help prevent future accidents such as the abuse of private data. Log records are legal proof of having trained the individuals listed under the privacy laws and regulations. And those who violate rules or attempt to harm actives will put a system administrator onto penalties associated with violating the law.

4. Prototype Implementation and Performance

4.1. Algorithm

Our proposed system can play an important role in protecting the HR data of the target company's employees held on M&A transactions. Based on the system described in the previous section, we design the mechanism for the main composition module; this must be controlled to secure access to authorized users. It is also reasonable to transfer or disclose the personal information in its control with consent, given in the prescribed manner. The algorithm for our proposed SIMS is shown below. We present an algorithm to decide to access based on policy, and to apply the result of processing to decisions.

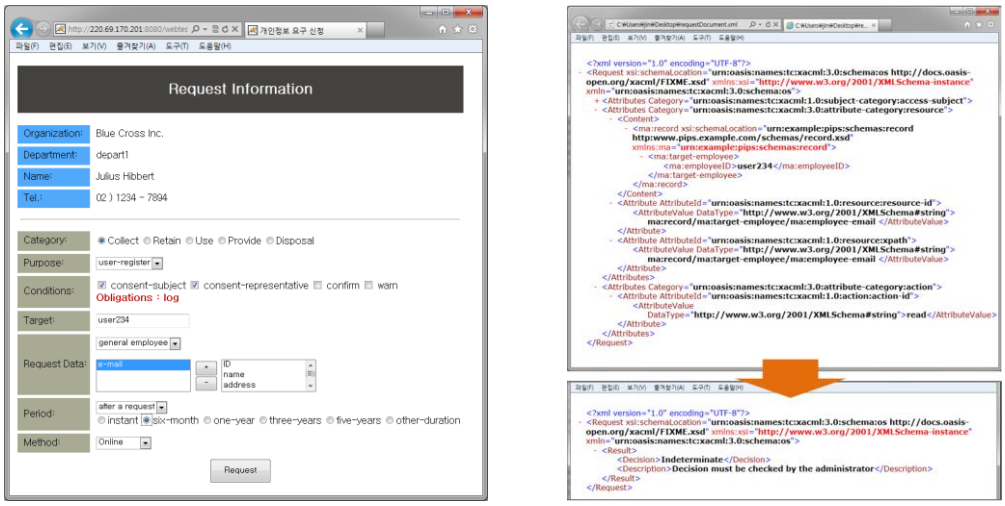
```
Algorithm
(1)   u ← a user who accessed the personal information;
(2)   k ← PIN generation key;
(3)   IF isAuthorized(u, generatedPIN(k)) THEN
(4)       IF haveRequired(u) THEN
(5)           request_doc ← convertXACML(u, request_info);
(6)           IF isValidated(request_doc) THEN
(7)               attr ← extractAttr(request_doc);
(8)               result ← checkupAttr(attr.subject_id, attr.access_purpose);
(9)               IF result = Deny THEN
(10)                  notifyUser(type:inform(Refuse));
(11)                  recordLog(reason, Timestamp);
(12)                  RETURN;
(13)              addHandlingFile(attr.subject_id, attr.access_purpose, attr.resource_id);
(14)              IF ( haveSensitivedata(attr.reource) OR
(15)                  result = {NotApplicable, Interminate} ) THEN
(16)                  IF haveCondition(attr) THEN
(17)                      response_decision ← execute(attr.condition);
(18)                  IF response_decision THEN
(19)                      result ← checkedByAdmin(attr);
(20)                      updateHandlingFile(result);
(21)                  ELSE
(22)                      notifyUser(type:inform(Refuse));
(23)                      recordLog(reason, Timestamp);
(24)                      RETURN;
(25)                  IF result = Permit THEN
(26)                      response_info ← dataRetrieval(attr.resource_id);
```

(27)	convertXACML(*u*, *response_info*);
(28)	**IF** haveObligations(*attr*) **THEN**
(29)	execute(*attr.obligations*);
(30)	recordLog(*reason*, Timestamp);

4.2. Prototype

To demonstrate the feasibility of our system, SIMS, which protects the personal information based on privacy policies, was developed using JSP and JAVA technologies. We use MySQL for our database server and Apache as the interface for the web server system. We designed a policy database, which manages privacy policies, and it is developed based on the laws related to privacy.

In its prototype, the Figure 4 below represents the example of a request. In Figure 4, (a) shows that user can request the personal details including name, DOB, financial status, and other particular entities. This request can convert a privacy policy language, known as XACML. (b) refers to the XACML policy to specify a request information, and verifies the result of processing applies to decisions in the system when any sensitive personal information is transferred or disclosed. In such case the decision must be checked again by the administrator.



(a) Detailed Information for request (b) Request and response policy

Figure 4. Prototype system

4.3. Simulation

We designed a program to simulate its performance: Privacy policies using XACML affect the response time perceived by the user. Therefore, the response time is the performance of the prototype system. By randomly processing the request, we compare the response time of two processing mechanisms, as shown in Figure 5. The lines on the graph represent the existing and proposed system response times. Compare to the existing system, the policy processing with XACML shows better performance, since XML based output reduces the time considerably during the process.

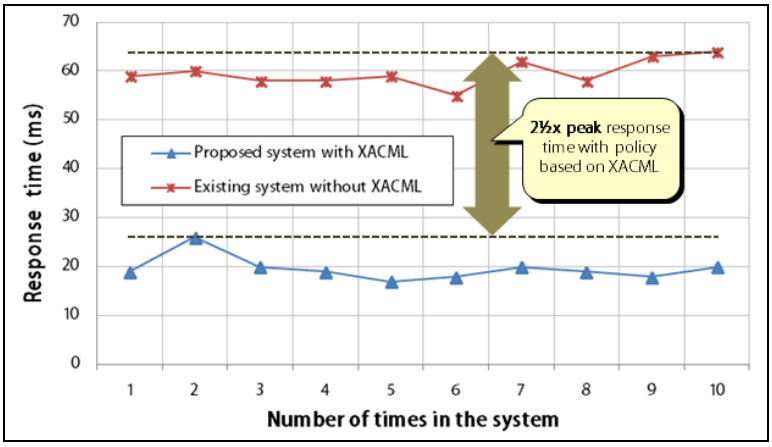


Figure 5. Performance evaluation of system prototype

5. Conclusion and Future Research

In this paper, we discussed privacy issues in an M&A transaction, and extracted problems. To address the privacy problems of an M&A process, we have proposed the SIMS for securely accessing and disclosing the sensitive personal information. Our system manages the private HR data based on privacy policies using XACML, and it supports evidence or a legal proof comply with the security laws. Our proposed system will play an adequate role of facilitating the protection of personal information in an M&A transaction.

In the future, we will focus our research on compliance issues in M&A activity, and continue to study the automated policy management for private data.

Acknowledgements

This work was supported by the Sungshin Women's University Research Grant of 2013.

References

[1] M. Borkowski, "Mergers and Acquisitions Privacy Risks", The Canadian Business Journal, **(2013)** February 13**.**

[2] M. J. Krasnow and A. York, "U.S. And Canadian Privacy Considerations for Mergers and Acquisitions", Mondaq News Alerts, **(2013)** June 4**.**

[3] J. -J. Kim and S. -P. Hong, "A Consolidated Authentication Model in Cloud Computing Environments", IJMUE, vol. 7, **(2012),** pp. 151-160.

[4] T. Burkhart, D. Werth and P. Loos, "Context-sensitive business process support based on emails", Proceedings of the 21st international conference companion on World Wide Web, **(2012)** April 16 - 20; Lyon, France.

[5] OASIS, eXtensible Access Control Markup Language (XACML) Version 3.0, **(2012)**

[6] S. Finkelstein and C. L. Cooper, "Advances in Mergers & Acquisitions", Emerald Group Publishing Limited, vol. 11, **(2012)**

[7] D. -H. Bae, "A Study on the Revision of the 'Personal Information Protection Act' and its Related Acts", IT & Law Research, vol. 6, **(2012).**

[8] Clyde and Co, "Corporate insurance: M&A activity A global overview 2009-2013, **(2013)** September 6**.**

[9] L. B. Erickson and E. M. Trauth, "Getting work done: evaluating the potential of crowdsourcing as a model for business process outsourcing service delivery", Proceedings of the 2013 annual conference on Computers and people research, **(2013)** May 30 - June 01; Cincinnati, OH, USA.

Authors

Kyong-jin Kim

He graduated with a B.S. in 2007, with a M.S. in 2009 and with a Ph.D. in 2013 from the Sungshin Women's University. She joined the Information Security lab as a postdoctoral fellow in March 2013. Her research interests focus on privacy protection, security framework, and access control.

Seng-phil Hong

He received his BS degree in Computer Science from Indiana State University, and MS degree in Computer Science from Ball State University at Indiana, USA. He researched the information security for Ph.D at Illinois Institute of Technology from 1994 to 1997, He joined the Research and Development Center in LG-CNS Systems, Inc since 1997, and he received Ph.D. degree in computer science from KAIST University in Korea. He is actively involved in teach and research in information security at Sungshin Women's University, Korea. His research interests include access control, security architecture, Privacy, and e-business security.