

Beyond Purpose-Based Privacy Access Control

Sabah S. Al-Fedaghi

Computer Engineering Department
Kuwait University
PO Box 5969 Safat 13060 Kuwait
sabah@eng.kuniv.edu.kw

Abstract

Research efforts have been directed toward the improvement of privacy protecting technology by incorporating privacy protection into database systems. Purpose acts as a central concept on which access decisions are made. A complexity of purpose and users role hierarchies is utilized to manage the mapping between users and purposes. In this paper, we propose a personal information flow model that specifies a limited number of acts on this type of information. Chains of these acts can be used instead of the "intended/business purposes" used in privacy access control.

Keywords: personal information, privacy, database system.

1 Introduction

Privacy is becoming an important feature in modern society. The rapid advances in information technology and the emergence of privacy-invasive technologies have made informational privacy a critical area to be protected. Personal information is used in making decisions about an individual's life. Regulations and laws have been established to allow people to control the way in which their personal information is used. Guidelines such as the 1980 OECD guidelines, legislation such as the Health Insurance Portability and Accountability Act (HIPAA) and systems such as P3P are not sufficient to safeguard privacy because "they do not address how personal data is actually handled after it is collected ... Privacy protection can only be achieved by enforcing privacy policies within an organization's online and offline data processing systems" (He et al., 2003). Also, "privacy cannot be efficiently implemented solely by legislative means. Data protection commissioners are therefore demanding that legal privacy requirements should be technically enforced and should be a design criteria for information systems." (Fischer-Hübner and Ott, 1998)

Privacy-enhancing technology aims at making privacy protection guidelines and laws an integrated part of the technology. Thus, an information system is designed to embed components that allow monitoring compliance of the system to privacy rules.

The notion of *Purpose* is the basic concept on which decisions to access personal information are made. A complexity of purpose hierarchies and users' role hierarchies are utilized to manage the mapping between users and purposes. We propose a personal information flow model that specifies acts on this type of information. Chains of these acts can be used to control acting on personal information instead of purposes used in privacy access control. The method is distinguished by the limited number of acts that form chains of acts on personal information.

2 Related Works

The Platform for Privacy Preferences (P3P) provides means for policy privacy specification and exchange but "does not provide any mechanism to ensure that these promises are consistent with the internal data processing." (Byun et al., 2005) Hippocratic databases have been introduced as systems that integrate privacy protection within relational database systems (Agrawal et al., 2002). A Hippocratic database includes privacy policies and authorizations that associate with each attribute and each user the usage purpose(s).

Privacy protecting access control deals with privacy policy specification and private data management systems. In privacy protecting access control models, "the notion of purpose plays a central role as the purpose is the basic concept on which access decisions are made" (Byun et al., 2005). "Most privacy-aware technologies use purpose as a central concept around which privacy protection is built." (Massacci et al., 2005)

Example: (from Byun et al. (2005)) Sample purposes defined on a given hierarchy of purposes are:

Allowable purposes = {Admin, Profiling, Analysis} \cup {Direct, D-Email, D-Phone, Special-Offers, Service-Updates}

Prohibited purposes = {D-Email, Special-Offers, Service-Updates} \cup {D-Email, Direct, Marketing, General-Purpose}

An access is granted if the access purpose (stated by user) is entailed by the allowed purposes and not entailed by the prohibited purposes (Byun et al., 2005).

Users role hierarchies similar to ones used in security policies (e.g., RBAC: Role Based Access Control mechanisms (Sandhu et al., 2000)) are used to simplify the management of the mapping between users and purposes. A request to access to data is accompanied by access purpose, and accessing permission is determined

after comparing such a purpose with the intended purposes of that data in privacy policies. Each user has authorizations for a set of access purposes.

Nevertheless, the management of attributes and users purposes is a complicated issue. Attributes and users purposes form hierarchies of the generalization and specialization (email marketing and telephone marketing is generalized as marketing) that are organized according to users' roles. To simplify the mapping process users are assigned roles, and access purpose permissions are granted to roles associated with tasks or functionalities, not directly to individual users (Byun et al., 2005). To support dynamic changes in purposes, "role" may be assigned attributes with hierarchy inheritance characteristics "to assign an access purpose to a specific subset of users in the same role" (Byun et al., 2005).

Purpose management introduces a great deal of complexity at the access control level. In this paper we introduce an alternative privacy access control mechanism that is not based on purpose.

3 Purpose

The notion of *purpose* appears in all privacy codes and legislations. For example, the Data Quality Principle in the OECD guidelines specifies:

Personal data should be *relevant* to the *purposes* for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date. (OECD, 1980)

Purposes are usually categorized into two types:

Consumer data purpose: This purpose expresses how the collected data can be used. P3P (2002) specified purposes include: Web Site and System Administration, Research and Development, Individual Decision, Contacting Visitors for Marketing of Services or Products, Historical Preservation, Telephone Marketing, and profiling.

Business purpose: This purpose is for business actions that involve certain consumer data operations.

Customer purposes are typically mapped to the more specific business purposes. For example, telemarketing is mapped to direct telemarketing and third party telemarketing and these in turn may be categorized into email telemarketing and telephone telemarketing such that the relationship among purposes modelled as a purpose hierarchy.

"A purpose specifies the intended use of the data element" and it "describes the reason(s) for data collection and data access" (Byun et al., 2005). Privacy policies utilize purposes in their accessing Personal Information (PI) mechanism.

Nevertheless, *purpose* remains a semantic concept that is "pasted" superficially to personal information. To utilize it in privacy protecting access control, we identify the relationship between purposes in order to build a hierarchy of purposes that tells us such things as which purpose-based access control is embedded into a more

general purpose control. This method is basically a privacy-covered version of a security access control mechanism. For the system, *purposes* could be described as "level 1," "level 2," ... instead of as Administration, Profiling, and Analysis, and it would not make any difference.

Instead, we propose to define the intended purpose of personal information as a chain of acts on this type of information. For example, the purpose could be:

Collecting (act 1) personal information, processing (act 2) it, in order to create (act 3) new information (e.g., *John is a risk*), to be used (act 4) in deciding a loan.

We claim that the number of types of acts on personal information is limited. In this case a chain of acts are permitted and other chains are prohibited. The chain represents a syntactical form of controlling access (acts in general) to personal information.

4 Personal Information

This section reviews the definition of personal information (PI) and its flow model given in Al-Fedaghi (2006a) and Al-Fedaghi (2006b).

4.1 Definition of personal information:

Personal information theory assumes two fundamental types of entities: *Individuals* and *Non-individuals* (Al-Fedaghi, 2005a and 2005b). The term *Individuals* represents the set of natural persons and *Non-individuals* represents the set of non-persons. *Personal information* (PI) is any linguistic expression that has referent(s) in *Individuals*. Assuming that p is a sentence such that X is the set of its *referents*, then there are two types of PI:

(1) p is the atomic personal information if $X \cap Individuals$ is the singleton set $\{X\}$. That is, atomic personal information is an assertion that has a single human referent (e.g., *John is 25 years old*). "Referent," here, implies an identifiable (natural) person.

(2) p is the compound personal information if $X \cap Individuals$ is a set of more than one person (e.g., *John loves Mary*). That is, compound personal information is an expression that has more than one human referent.

The relationship between individuals and their own atomic personal information is called *proprietorship*. If p is a piece of atomic personal information of $v \in Individuals$, then p is proprietary personal information of v , and v is its *proprietor*.

A single piece of atomic personal information may have many possessors; where its proprietor may or may not be among them. A *possessor* refers to any entity that knows, stores, or owns the information. Any compound personal statement is privacy-reducible to a set of atomic personal statements.

Personal information privacy involves acts on personal information in the context of creating, collecting, processing, and disclosing this type of information.

4.2 Personal Information Flow Model:

The personal information flow model divides functionality into four modules or phases that include informational privacy entities and processes, as shown in Figure 1.

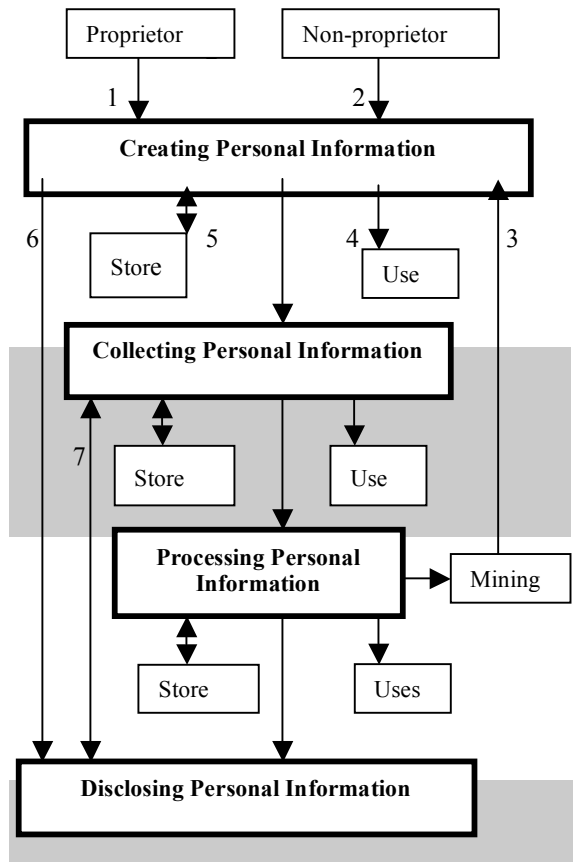


Figure 1: Personal information flow model.

New PI is created at Points 1, 2, and 3 by proprietors or non-proprietors (e.g., medical diagnostics by physicians), or is deduced by someone (e.g., data mining that generates new information from existing information). The created information is used either at Point 4 (e.g., decision making), Point 5 (stored), or Point 6, where it is immediately disclosed. Processing the personal information phase involves acting (e.g., anonymization, data mining, summarizing, translating) on PI. The disclosure phase involves releasing PI to insiders or outsiders. The “disposal” or disappearance of PI can happen anywhere in the model, such as in the transformation to an anonymous form in the processing phase. “Store” in Figure 1 denotes both storing and retrieving operations.

Example: Consider the situation where we have one proprietor and two PI agents (e.g., companies, departments, agencies, other individuals). Suppose that the roles of these three actors are defined as follows:

Proprietor: Creates, stores, and discloses PI to Agent 1.

Agent 1: Collects, stores, uses, and discloses PI to Agent 2.

Agent 2: Collects and processes PI through a mining technique that creates new PI that is stored and used in some applications (e.g., decision making). The PI flow model for this simple environment can be drawn based on Figure 1, as shown in Figure 2.

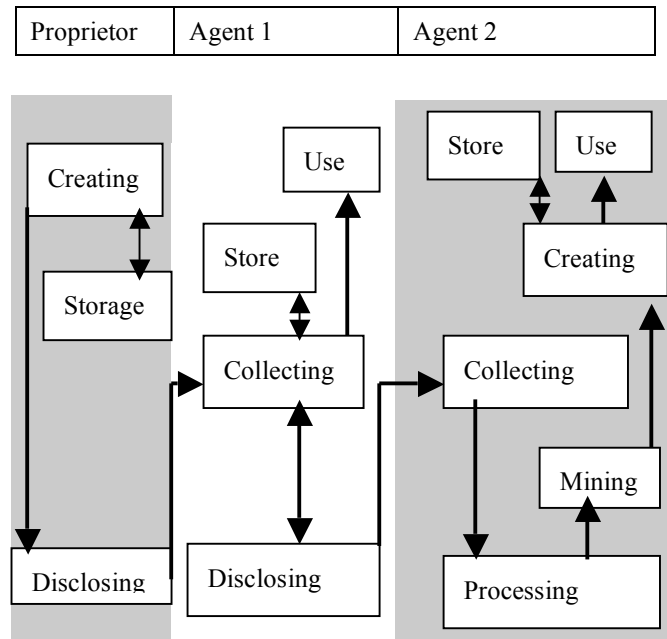


Figure 2: A proprietor and two agents model.

For each actor in this scenario we will make a copy of the PI flow model. However, because the proprietor does not collect or process PI, these phases are not shown in his/her region. The creation and processing phases are not shown for Agent 1 because it does not create or process PI. Similarly, the disclosure phase is not shown in the region of Agent 2. Let t be a piece of PI of the proprietor. It originates in the *Creating* box in the proprietor's region. It is stored in *Store*, and moves through the *Disclosing* box to the *Collecting* box of Agent 1's region. It is stored and used there, and moves through the *Disclosing* box to the *Collecting* phase of Agent 2. There, it moves to the *Processing* to the *Mining* boxes where it generates new PI in the *Creation* phase for storage and later use. We can add details to any phase as the situation requires. For example, Agent 2 may add *Store* to keep a copy of the original PI or a *Disclosure* phase can be added if Agent 2 discloses the resultant new PI to a third agent.

5 The Proprietor-Others Architecture

This section and Section 6 review with some additional materials the architecture given in Al-Fedaghi (2006a).

Using the PI flow model, we can build a system that involves a proprietor on one side and others (other persons, agencies, companies, etc.) who perform different types of activities in the PI transformations among the four phases of flow of personal information. We will refer to any of these as PI agents. PI agents may include any one who participates in activities over PI. The proprietor is not accepted as agent with respect to his/her own PI.

Figure 3 illustrates this type of mode of operation on PI with sample PI agents. The solid arrows reflect that the proprietor is a source of PI for agents. The dotted lines reflect that this PI of the proprietor may also be directly shared and exchanged among agents.

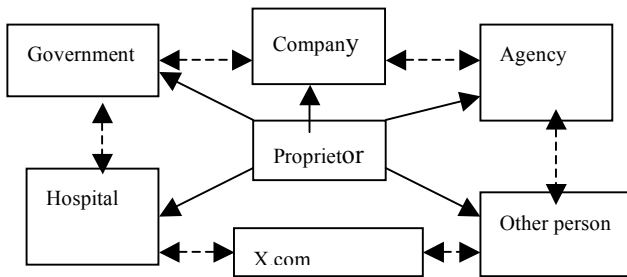


Figure 3. Proprietor/others PI exchange scheme.

The EU Privacy Directive manages this type of system: organizing (1) the relationship between the proprietor and agents that utilize his/her personal information and (2) the relationship among the agents.

According to the EU Directive (1995):

(25) Whereas the principles of protection must be reflected, *on the one hand*, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification

to the supervisory authority, and the circumstances under which processing can be carried out, and, *on the other hand*, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances” (Italics added).

Notice that this type of system is basically a “binary” system that involves the proprietor on one side and all agents, represented in the EU Privacy Directive by the “controller” on the other.

6 The Acts on the Proprietor’s PI

As a result, we need two *types* of PI flow models: one for proprietors and one for agents. We construct this proprietor/agent PI flow architecture with two regions: the proprietor’s region of activities on his/her PI and the others’ region of activities on the proprietor’s PI, as shown in Figure 4. Notice that we concentrate in the figure on the agent’s region. This region is a copy of the personal information flow model.

We assume that there is no interest in how a proprietor collect and process his own PI. For example, the EU Directive specifies that “there should be excluded the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses” (EU Directive, 12).

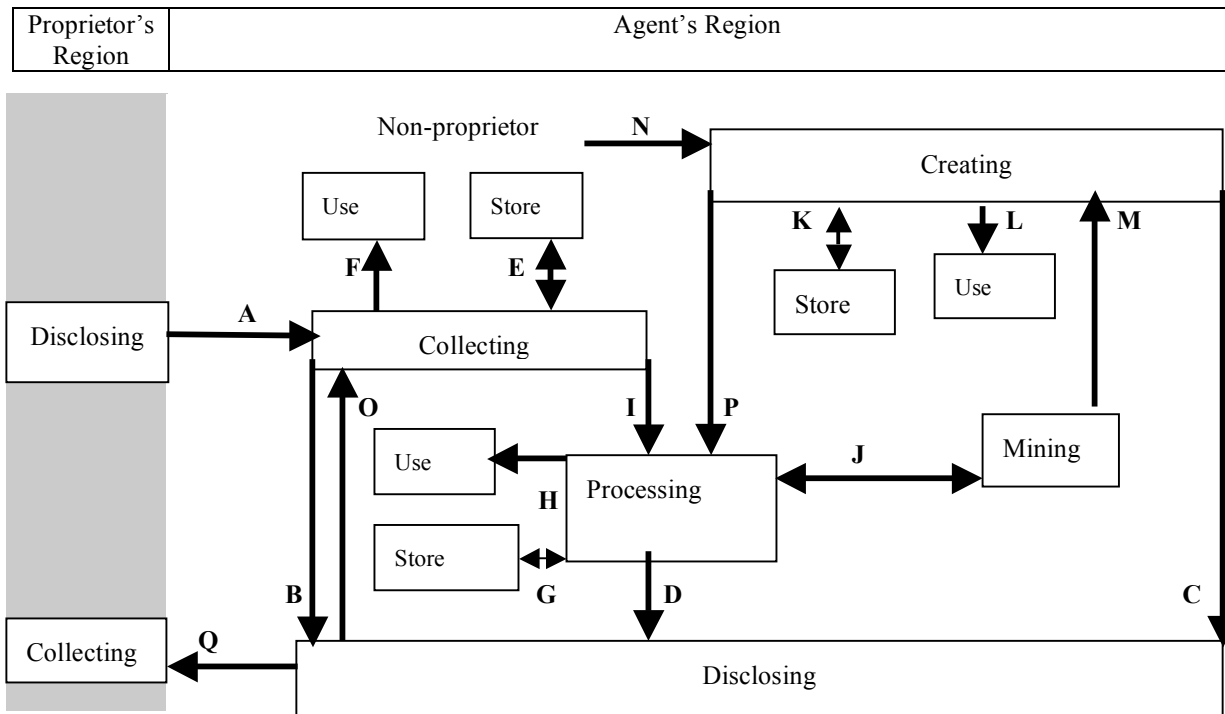


Figure 4. Architecture of Proprietor/Agent PI flow

We distinguish 17 types of acts on PI (labelled A through O) as shown in Figure 4 and described in Table 1. These acts form ordered sequences or chains as will be discussed later.

| Acts | Descriptions | Comments |
|------|-------------------------------------|--|
| A | Disclosing PI by a proprietor | Act A also represents collecting PI (by a collecting agent). |
| B | Disclosing PI by a collecting agent | B implies O (collecting PI by another collecting agent) |
| C | Disclosing PI by a creating agent | In Figure 4, C implies B, that is, the disclosed PI flows from a collecting agent to another collecting agent. |
| D | Disclosing PI by a processing agent | In Figure 4, D implies B, that is, the disclosed PI flows from a processing agent to a collecting agent. |
| E | Storing PI by a collecting agent | E (double arrow in figure 4) includes retrieval. of PI. |
| F | Using PI by a collecting agent | "Using" indicate non-informational operations. |
| G | Storing PI by a processing agent | We can separate the storing and retrieval acts as two independent acts in the model. |
| H | Using PI by a processing agent | Using processed PI may be different from uses of other types of PI. |
| I | Processing PI by an agent | PI flows from the collecting phase to a processing phase, assuming the same agent. |
| J | Mining PI by a mining agent | Mining is a type of processing (notice the bi-directional arrow). This type of mining (back arrow) produces implied PI but not new PI. |
| K | Storing PI by a creating agent | |
| L | Using PI by a creating agent | |
| M | Creating PI by a mining agent | Automatic creation of PI. Notice that mining is a special type of processing. |
| N | Creating PI by a non-proprietor | Non-automatic creation of PI (e.g., gossip). |
| O | Collecting PI from non-proprietor | O occurs simultaneously with B: If an agent discloses PI then there is an agent that collects that PI. |
| P | Processing of created PI | Non-proprietor may creates PI and process it immediately without storing or acting on it. |
| Q | Disclosing to proprietor | E.g., Informing a person of results of medical tests. |

Table 1. Acts on Personal Information

Examples:

Act A: A person discloses PI to a hospital.

Act B: A hospital discloses PI to an insurance company.

Act C: PI is produced by a mining program (e.g., *John is a high-risk customer*) of a bank is disclosed to crediting company.

Act D: Processed PI (changing the original data to another form through such operations as modification, translation, summarization, generalization) is released from a hospital to an insurance company.

Act E: A hospital stores PI in its automated or manual system, accessing stored data.

Act F: A hospital uses PI to contact its patients.

Act G: A hospital stores processed PI (e.g., mined PI) in its system .

Act H: An agent uses processed data for research.

Act J: An agent mines PI to extract implied PI (e.g., the information *Z is the grandfather of Y* is taken from *Z is the father of W* and *W is the father of Y*).

Act K: An agent stores PI produced by a mining program.

Act L: An agent makes decisions based on PI that is produced from a mining program.

Act M: An agent produces new PI using a mining program (e.g., an analysis of customers produces the information that *John is a high-risk person*).

Act N: A newspaper writer publishes PI.

Act O: An agent collects PI from another agent.

Act P: An agent creates PI (gossip) and processes it.

The advantage of this categorizing of "processing" of personal data is that we can specify different types of rules, requirements, restrictions for each type of act on PI (Al-Fedaghi, 2006a). The next section proposes to use the chains of acts on PI as a mechanism that is tied to the user purpose.

7 Chains of Acts on Personal Information

We have now a foundation for developing a purpose-less privacy protecting access control mechanism. We assume that each purpose can be translated to a chain of acts on PI. To simplify the discussion, the concept is introduced through known examples in the research literature.

Chains of acts on PI are chains of *information handling* that starts with one of the following acts:

Act A: A proprietor discloses his/her PI. This act can also be described as an agent collecting PI from a proprietor.

Act O: An agent collects PI from another agent. In this case O may be preceded by the act of disclosing agent to indicate where the PI coming from.

Act N: A non-proprietor creates PI.

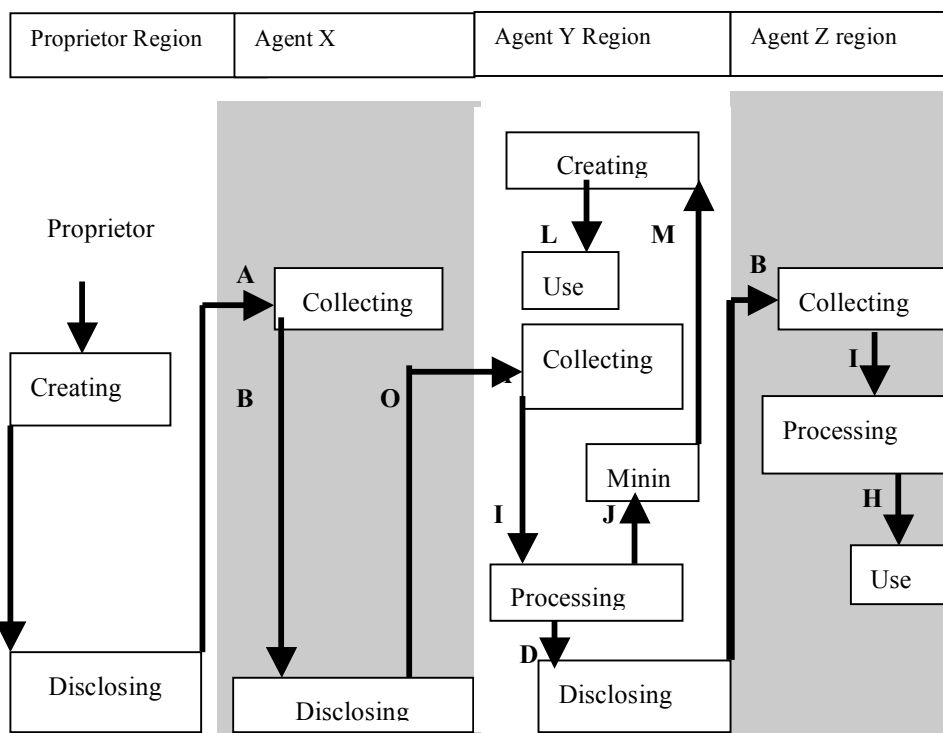


Figure 5. The architecture of the flow of PI for the given example.

These three acts, A, O, and N, are the only sources that supply any agent with PI. Suppose that a company has a piece of personal information. This piece of information is either collected from its proprietor, from another agent, or created internally by the agent. Starting with any of these sources, that piece of PI flows into the PI information handling system (manual or automatic) subjected to different acts such as processing, utilization, mining and so forth. This track of acts can be traced through *chains*.

One benefit of these chains is designing the PI handling system such that each piece of PI is constrained to flow in specific chains.

Example: Suppose that a company collects PI from proprietors and utilizes it in direct email telemarketing. The chain of acts that describes the flow of PI in this operation is AF (the sequence starts with act A then act F) which includes:

Act A: Collecting PI from a proprietor

Act F: Using PI in direct telemarketing operation

If the company also stores the PI (act E: Storing and retrieving) then we have two possibilities:

(1) PI is collected, stored, then used in telemarketing. The chain AEF represents this sequence of acts.

(2) The PI is collected and utilized directly in telemarketing, and in parallel stored and utilized later in telemarketing. This is represented by the chains AF and AEF. AF and AEF are two paths of flow of information, one is directly from collecting to telemarketing and the other goes from *Collecting* to *Store* to *Use*.

Suppose that the company also use the PI for third party marketing (i.e., it sells the PI to another telemarketing company). In this case, samples of possible chains:(1)

AB: Disclosing PI straight to the other agent without using it itself in telemarketing.

(2) Two chains, AB and AF: Disclosing PI to the other agent and using it in its own telemarketing. A sample situation that reflects AB is the following: a customer requests PI about a certain person from a private investigation agency under the condition that the agency does not keep records of PI after delivering it to the requester.

(3) Two chains, AEF and AEB: Storing PI and using it, and also disclosing PI to the other agent.

These types of acts on PI represent constraints on methods of handling PI. The "enterprise purpose" is represented by a set of these chains.

Example: Consider a proprietor, X, and two agents, Y and Z. Assume that the flow of information reflects the following *roles* for agents:

Proprietor: discloses his/her PI to collecting agent Y

Agent X: collects PI of X and discloses it to Agent Z.

Agent Y: collects PI from Agent X and processes it through a data mining program that creates new PI which is used in decision-making (e.g., denying a loan).

Agent Z: Collects PI from Y and processes it to use the results in research.

Figure 5 shows the architecture of the flow of PI in such a system.

| | Possible chain of acts | Examples | Explanations |
|---|------------------------|--|---|
| 1 | A | Collecting PI to satisfy curiosity without storing, using, or disclosing it. | The purpose of act A alone without being followed by storing, using, or disclosing the PI is a "mere collecting" act. |
| 2 | A then B | Selling PI to agent Y | Collected PI is immediately disclosed to another agent. |
| 3 | A then E then B | Selling PI to agent Y while keeping a copy of it | As when a telemarketer uses PI and also sells it to others. |
| 4 | A then E | Just storing collected information. | As in archival storage where data <i>may</i> never be needed. |
| 5 | A then F | Direct use of PI without storing it | |
| 6 | A then E then F | Storing PI then using it | |
| | B... | The flow of PI starts from an origin that creates it. These chains are illegal because they should start with A (PI is created by its proprietor), M (PI is manually created by a non-proprietor), or N (PI is automatically created by a non-proprietor). | |
| | E... | | |
| | F... | | |

Table 2. Six possible chains that can be assigned to X.

Chains of X: Table 2 shows six possible chains that can be assigned to X. Notice that a sequence such as AFB is not mentioned because it means that the agent collects PI then used (act F), and disclosed (act B) it. Acts F and B are not dependent (in the flow of PI) on each other, hence, we can write them in terms of the two basic sequences: AF and AB.

In our example, by assumption, Agent X does not merely collect PI, neither *store* nor *use*. The only chain used by X is AB. We can observe here that such categorization of utilization of PI is based on purely syntactical consideration (the 17 acts and the relationships among them) and does not depend on any particular situation.

Chains of Y: Possible chains that are applied to Agent Y are: B, BI, BIJ, BIJM, BIJMN, and BID. However, according to our example Agent Y use only the chain BIJM.

Chains of Z: Possible chains that are applied to Agent Z are: B, BI, and BIH.

Suppose that all three agents are in the same enterprise. Then the enterprise system can organize the activities of these agents such that each is constrained to a certain chain. For example, X is not permitted to access PI produced by the mining program, Y is not permitted to disclose PI to X, Z is not permitted to disclose PI to anyone.

8 Privacy Access Control

We are proposing to use chains of acts on PI to control acting on PI instead of the so-called "business purposes" used in privacy access control.

Example: This example is a revised version of Byun et al. (2005). Suppose that we wish to allow three types of users:

E-Analysts are the users who analyze the customer information and prepare the contents of emails. They have the permissions to access the customer profiles.

Writers are the users who write and send out emails to customers. They have the permissions to access the email addresses of the customers.

Service-Update refers to workers who send out updated service information and then update the information.

In this scenario, we have three agents, the proprietor and the system as an agent. The *system* represents the total information system that the three agents are its users. The chains for each agent are as follows, where we specify only the relevant acts (qualified with "" for the system):

System: B', O'G': These are the required acts from the system in the context of the example: B' (disclosing PI) which refers to provide viewing (access) of PI to other agents; and O'G' (collecting PI released by other agents and storing it).

E-Analysts: B'OIBO'G': That is, collecting PI from the system (B'O), processing (altering) it (I), and disclosing it to the system (O') to be stored back (G').

Writers: B'OF: That is, collecting PI from the system (B'O) and use it to send out emails to customers. We assume that sending out emails to customers is one of the uses (Use box).

Service-Update: Includes two chains:

a) B'OF: That is, collecting PI from the system (B'O) and using it to communicate with the customers to update their PI.

(b) ABO'G': That is, collecting the updated PI from customers (A) and disclosing (releasing) it to the system (BO') to be stored back.

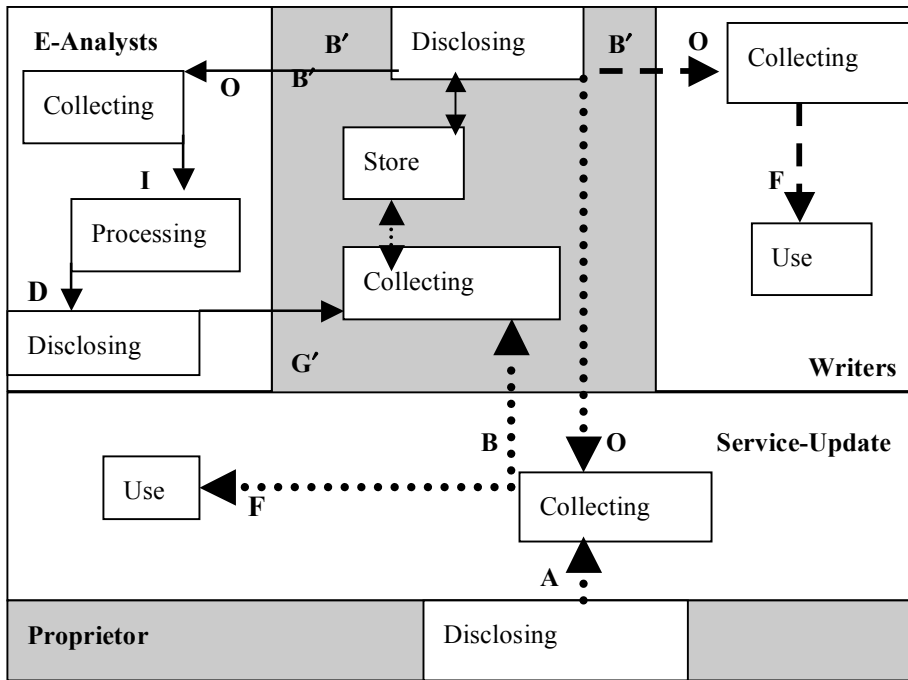


Figure 6. Chains of three agents, the proprietor and the system.

Figure 6 shows the PI flow models for the three agents, system, and proprietor. Each chain in this case is a constraint on its relevant PI: email of Writers, profile of E-Analysts, and the PI relevant to the Service-Update workers.

This methodology is an alternative method to *enterprise purpose* and roles hierarchies. Each PI is associated with a chain that reflects permissible acts to accomplish the *customer purpose*. If the purpose is *direct email telemarketing* then the chain OF is associated with the email information. The users (e.g., Writers in the example) in this case can only collect the email information and use it to send out emails to customers. We assume that there is a system application program that is designed to send out these emails to customers. The chain OF is implemented by programs that allow these users to access the email information. This mapping between chains and users is a replacement of the mapping between purposes hierarchies and users roles hierarchies.

9 Architecture for Personal Information Database System

The high level description of architecture for a personal information database system will be referred to as PIDB.

PIDB is formed from regions for proprietors and agents. Each region is a copy of the PI flow model as described previously.

Example: This example is a revised version of Massacci et al. (2005) who built it from the case study proposed by Agrawal et al. (2002).

Mississippi relies on Worldwide Express (WWE) for shipping books. WWE is a delivery company that offers a global network of specialized services – transportation, international trade support and supply chain services. WWE also needs personal information to deliver books for Mississippi. This information includes customer name and shipping address. In turn, WWE depends on local delivery companies for door-to-door delivery. To this end, WWE delegates customer information to them. Furthermore, Mississippi relies on the Credit Card Company (CCC) for credit assessment. CCC needs to obtain some information for providing credit assessment. This information includes customer's name and credit card number, and the transaction between Mississippi and the customer. For making credit decisions, CCC wants a credit rating. For this, CCC depends on the Credit Rating Company (CRC). CRC uses statistics to summarize past experience so that predictive analysis can be used to generate a rating for the customer. Based on the rating, CCC can decide to accept or not the customer transaction.

This scenario includes one (type of) proprietor and six agents as illustrated in Figure 7. The figure shows the relationships between these acts. Mississippi has two internal users.

Figure 8 shows the architecture of PIDB for the actors Proprietor, Mississippi, Credit Card Company, Worldwide Express and Local delivery companies. The flow model of the internal departments can be specified in similar way to the agents E-Analysts, Writers, and Service-Update in the example in the previous section. For example, the chain from ordering books to delivering it to customer is described in the following chains:

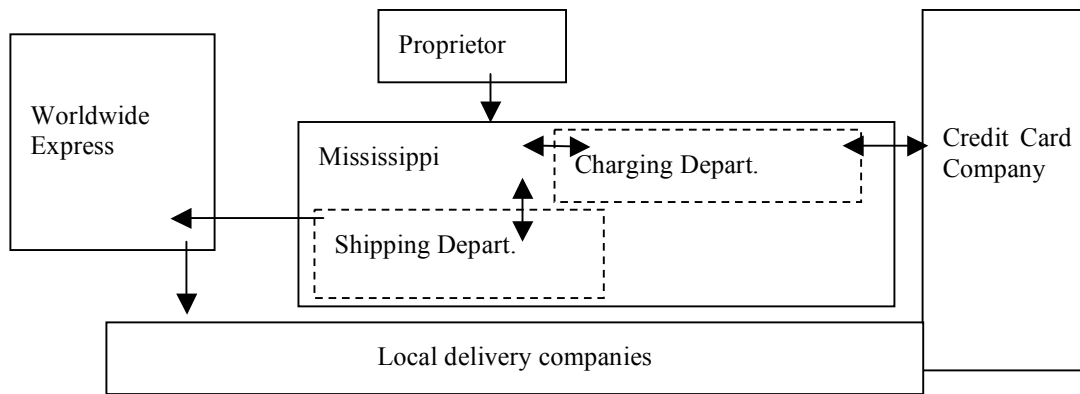


Figure 7. General view of the relationships among six acts in the Mississippi example.

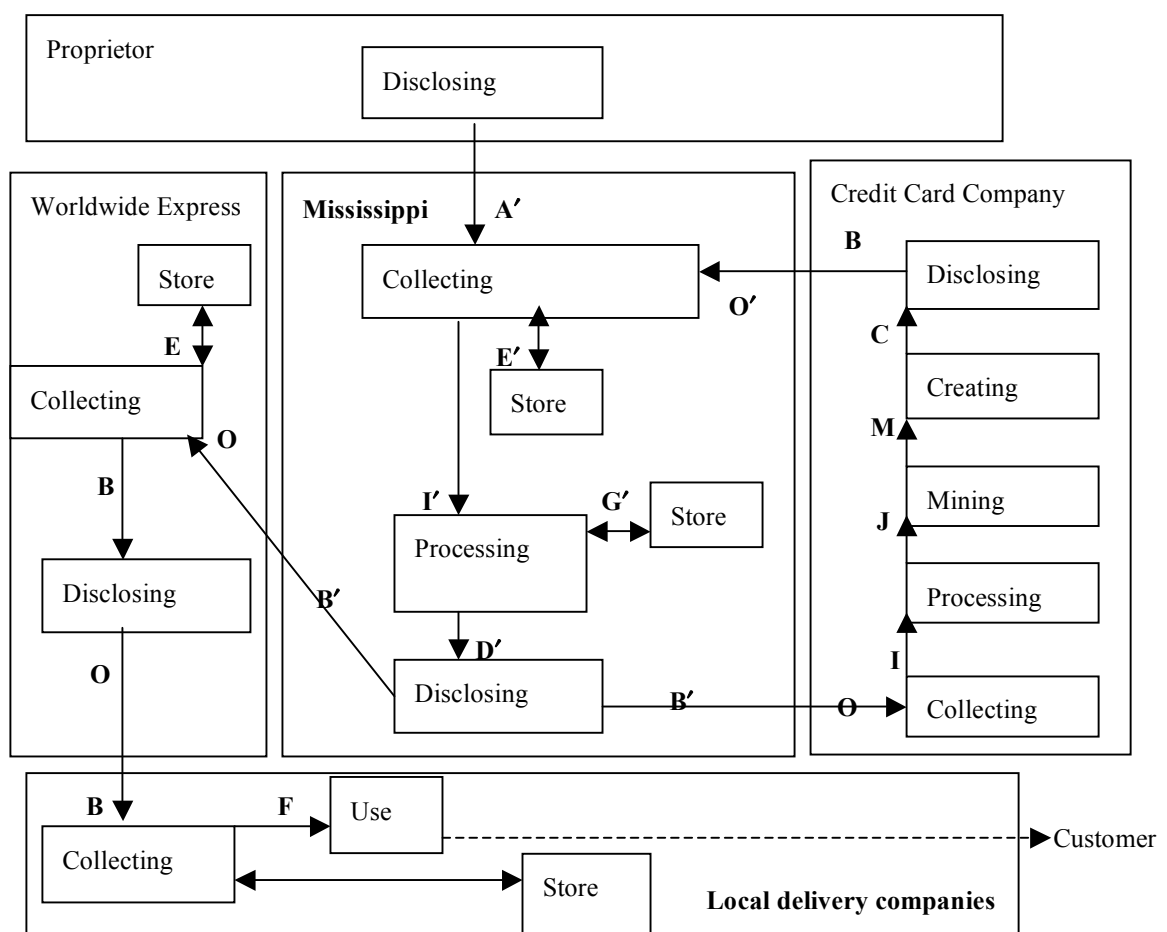


Figure 8. The architecture of PIDB for the Mississippi example.

Mississippi: A' E' I' G' D' B'

Mississippi collects PI from customer, stores, process, stores (any results from processing), release PI to be disclosed to the Credit Card Company.

Credit Card Company: OIJMCB

Credit Card Company collects PI (from Mississippi), process, mine, release (new PI, e.g., John's credit is OK), and disclose it to Mississippi

Mississippi: O'I'D'

Mississippi collects results, process, and send delivering order to Worldwide Express (Assuming, credit is OK).

Worldwide Express: OEBO

Worldwide Express collects PI, stores, and discloses it to Local delivery companies.

Local delivery companies: BEF

Local delivery companies collect PI, store and perform the actual act of delivering the purchase.

As we see that other chains can be added to this scenario. Privacy Constrains can be supper imposed on internal or cross-organizational handling of personal information. The method is distinguished by the limited number of acts that form well defined chains of acts on personal information. In comparison with the complexity of hierarchies of purposes and roles and the mapping between them this method promises an attractive alternative. Additionally, the method is a manifestation of the notion "privacy by design" that embeds privacy constrains inside the system.

Figure 9 shows all possible chains of acts. PI entry points are acts A, B, and N. It generates non-informational acts (e.g., decisions) at F, H, and L. The dotted line between B and O indicates simultaneous acts (disclosure and collection) of two different agents as described previously.

10 Conclusion

The concept of representing database system's privacy constrains as chains of acts on personal information has been shown to be a possible alternative method to database techniques based on purpose hierarchies. A great deal of investigation is needed to formalize and experiment with such a mechanism. The general method has more applications than mere privacy protecting access control method. It can additionally be applied in writing privacy codes, guidelines, and statutes (Al-Fedaghi (2006c)).

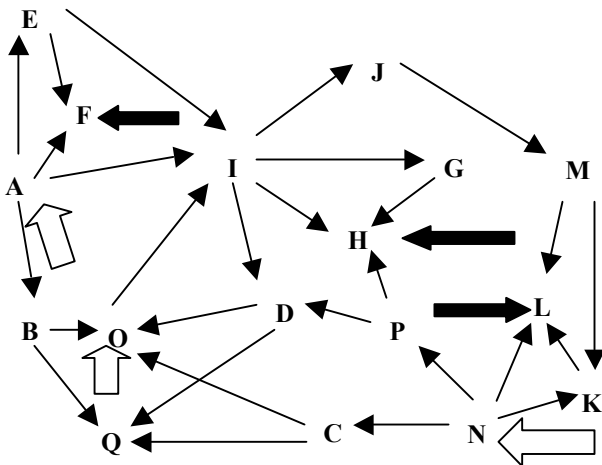


Figure 9. Acts sequences. Wide blank arrows are PI entry points and wide black arrows are uses where PI generates non-informational acts.

11 References

Agrawal, R. Kiernan, J. Srikant, R. and Xu. Y. (2002). Hippocratic databases. In The 28th International Conference on Very Large Databases (VLDB), Hong Kong, China, August.

Al-Fedaghi, S. (2006a) Anatomy of Personal Information Processing: Application to the EU Privacy Directive, International Conference on Business, Law and Technology (IBLT 2006), Copenhagen on December 5-7, 2006.

Al-Fedaghi, S. (2006b). Aspects of Personal Information Theory, 7th, The Seventh Annual IEEE Information Assurance Workshop (IEEE-IAW), West Point, NY: United States Military Academy, June 20-23.

Al-Fedaghi, S. (2006c). Personal Information Flow Model for P3P, *W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement*, Ispra (Italy), 17-18 October 2006

Al-Fedaghi, S. (2005a). How to Calculate the Information Privacy, The Third Annual Conference on Privacy, Security and Trust, St. Andrews, New Brunswick, Canada.

Al-Fedaghi, S. Fiedler G. and B. Thalheim B. (2005). Privacy Enhanced Information Systems, Proceedings of The 15th European-Japanese Conference on Information Modeling And Knowledge Bases: Tallinn, Estonia, 2005.

Byun, J. Bertino, E. and Li, N. (2005). Purpose Based Access Control of Complex Data for Privacy Protection, SACMAT'05, June 1-3, 2005, Stockholm, Sweden.

EU Directive. (1995). DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 24 October. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>

Fischer-Hübner, S. and Ott, A. (1998). From a Formal Privacy Model to its Implementation, Proceedings of the 21st National Information Systems Security Conference, Arlington, VA, October 5-8, 1998.

He O. and Antón. A. I. (2003). A Framework for Modeling Privacy Requirements in Role Engineering, International Workshop on Requirements Engineering for Software Quality (REFSQ 2003), Klagenfurt / Velden, Austria, 16 - 17 June, 2003.

Massacci, F. and Mylopoulos, J. and Zannone, N. (2005) Minimal Disclosure in Hierarchical Hippocratic Databases with Delegation. 10TH EUROPEAN SYMPOSIUM ON RESEARCH IN COMPUTER SECURITY, Milan, Italy - September 12-14, 2005.

OECD (1980). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

P3P (2002). The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, The World Wide Web Consortium, April 16, 2002, <http://www.w3.org/p3p/>.

Sandhu, R. Ferraiolo, D. and Kuhn, R. (2000). The NIST model for role-based access control: Towards a unified standard. In the fifth ACM workshop on Role-based access control, July 26-27, 2000.