USING OBJECT-ORIENTED CONCEPTS TO DEVELOP A CONCEPTUAL MODEL FOR THE MANAGEMENT OF INFORMATION PRIVACY RISK IN LARGE ORGANISATIONS

Kamil Reddy and H.S. Venter

Information and Computer Security Architecture Research Group
University of Pretoria

{kreddy, hventer}@cs.up.ac.za

ABSTRACT

In this paper we present a conceptual model for the management of information privacy risk in large organisations. The model is based on the similarities between the concepts of departments in large organisations and the object-oriented computer programming paradigm. It is a high-level model that takes a holistic view of information privacy risk management, and, as such, identifies risk in both manual and automated processes during the acquisition, processing, storage and dissemination of information. While conceptual in nature, the model is well suited to practical implementation due to the structure it derives from the object-oriented paradigm. The practical application of the model is demonstrated by way of an example scenario.

This paper contributes by addressing the absence in the literature of freely available models for the holistic management information privacy risk in large organisations.

KEY WORDS

Information Privacy, Information Privacy Risk, Information Privacy Management

USING OBJECT-ORIENTED CONCEPTS TO DEVELOP A CONCEPTUAL MODEL FOR THE MANAGEMENT OF INFORMATION PRIVACY RISK IN LARGE ORGANISATIONS

1 INTRODUCTION

Many organisations acquire, store, process or disseminate information related to individuals. These organisations are often bound by law [1, 2] to protect the interest individuals have in accessing, controlling, or significantly influencing, the veracity and use of their information. This interest is termed *information privacy* [3]. Where information privacy is not adequately protected by an organisation, affected individuals may seek legal recourse against the organisation. This may result in the organisation suffering financial loss and damage to their reputation. *Information privacy risk* (IPR) is the collective term for risks that lead to such breaches of information privacy.

Large organisations generally require a more coordinated and formal approach to their operations than smaller ones [4, 5]. The effective management of IPR in large organisations is therefore particularly important. In this paper, we present a high-level conceptual model that can be used to assist in the management of IPR. As it is a high-level model, it is designed for use by those charged with the overall management of privacy protection within an organisation or department. The model is based on the similarities between departments in large organisations and the object-oriented computer programming paradigm. It is holistic because it addresses IPR in both manual and automated processes during the acquisition, processing, storage and dissemination of information. In order to address the various types of information privacy breaches, the model makes use of the Organisation for Economic Cooperation and Development's Guidelines on the Protection of Privacy and Transborder

Flows of Personal Data (OECD guidelines) [6]. The OECD guidelines set out principles for the ethical handling of private information. The principles contained in the OECD guidelines form the basis of information privacy law in most countries [7, 8].

The rest of this paper is structured as follows. Section 2 describes the related work in the literature. Section 3 provides background on the object-oriented programming paradigm and the OECD guidelines. It also defines what we term the object analogy. The model is described in Section 4. A hypothetical scenario that uses the model is provided in Section 5. Section 6 consists of a discussion of the model. The paper is then concluded in Section 7.

2 RELATED WORK

In this section we discuss the related work found in our review of the literature.

Our search of the literature revealed only a single example of a privacy management model. This model, called *Privacy by 3PT*® [9], is the proprietary work of a company called the Corporate Privacy Group and is hence not freely available for use or public scrutiny. As such, it was not possible to analyse the model in detail. From the company's own literature on the model [9], it focuses on people, policies, procedures and technologies as distinct areas of concern. We do not devote further attention to the details of this model due to the lack of publicly available information. From the information that is available, our model differs in its areas of focus. Our model is also less prescriptive with regard to implementation steps and methods.

Karjoth and Schunter [10] developed a privacy policy model for the specification and enforcement of organisation-wide privacy policies. Their work was extended to form IBM's Enterprise Privacy Authorization Language (EPAL) [11]. EPAL is a formal language and is concerned with the enforcement of policies within information technology (IT) systems [11]. Our work differs from EPAL because our work is applicable at a higher level, and is not concerned only with IT systems.

® 'Privacy by 3PT' is a registered trademark of the Corporate Privacy Group

Casassa Mont [12, 13] also addresses the management of private information in organisations through the use of privacy obligations. *Privacy obligations* are policies that specify the duties and expectations under which organisations must manage private information [12]. Although privacy obligations are considered in EPAL, he develops them in greater detail [13]. Casassa Mont's work is also at the system level and therefore different to our approach.

Biskup and Brüggemann [14, 15] developed DORIS (*Datenschutz-orientiertes Informationssystem*). DORIS is a prototype implementation of a system based on *The* P*ersonal Model of Data*, a model also developed by Biskup and Brüggemann [14, 15]. In The Personal Model of Data the world consists only of entities called 'persons*'*. '*Persons*' represent individuals in the real world. DORIS uses objects to represent 'persons'. The objects consist of attributes and methods. Attributes correspond to an individual's knowledge of themselves in the real world. Methods correspond to actions taken by the individual in the real world. Biskup and Brüggemann also develop a data model, data manipulation language and rights-based privacy policy that are used in the DORIS system. We do not elaborate on these due to space restrictions.

Our work is similar to that of Biskup and Brüggemann in that we also make use of objects. It differs, however, because we make use of similarities between the concepts of organisational departments and objects, while Biskup and Brüggemann uses objects to model individuals. In our work we also go into greater detail regarding the object metaphor. Unlike our work, which is a high-level model, theirs is restricted to enforcing privacy within a single system. Another significant difference is that Biskup and Brüggemann take a view of privacy that is limited to ensuring appropriate access to private information. Their work does not consider the other aspects of information privacy as espoused in the OECD Guidelines.

3 BACKGROUND

In this section we present the background necessary to understand our model and the rationale behind it. We discuss the object oriented programming paradigm, organisational departments, the object metaphor and the OECD guidelines.

3.1 The Object-Oriented Programming Paradigm

We divide our discussion of object-oriented programming (OOP) paradigm into a discussion of the concepts behind the paradigm and brief example of how it is used.

3.1.1 Defining OOP Concepts

There is no single set of concepts that is universally accepted as making up the OOP paradigm [16]. It is, however, most commonly characterised as consisting of three concepts: objects, classes and inheritance [17]. An *object* can be defined as "an individual, identifiable item, either real or abstract, which contains data about itself and descriptions of its manipulations of the data" [16]. The data contained in an object are called *attributes*, while the manipulation of the data is achieved through *methods*. An object's *set* methods are used to input data or to change existing data in the object. An object's *get* methods, on the other hand, may used by other objects to retrieve data from the object.

The concept of *encapsulation* ensures that access to an object's attributes and methods from 'outside' the object is strictly limited according to the definition of each attribute and method. We mention encapsulation in addition to the three concepts listed above because it is also often associated with the OOP paradigm [16] and it is relevant to our model.

We use the definitions in Armstrong [16] to define a *class* as an abstraction of an object that defines the common structure and behaviour shared by a set of objects. An object which belongs to a class is thus a 'concrete' instance of the class. The verb *instantiate* is used to denote the creation of an object from a class definition. *Constructors* are special methods used to instantiate objects. Attribute values may be set at the time of instantiation using a constructor. The accessibility of an object's attributes or methods, required for encapsulation, is specified in an object's class definition.

3.2 The Object Analogy

In a large organisation private information is typically used by one or more departments, for example, the finance and marketing departments. In each department the information may be stored as well as manipulated. By manipulated we mean received, processed, disseminated or any combination thereof. Departments generally also use a fixed number of known methods for storing and manipulating information. This is analogous to an object in the sense that information in an object can be stored using attributes, and manipulated using methods. The direct analogy between objects and departments is termed the *object analogy*. The object analogy is illustrated in Table 1.

Table 1 – The Object Analogy

Department	**maps to**	**Object**
Type of department	→	Class
Department	→	Object
Information	→	Attributes
Receipt of information	→	Get and set methods, constructors
Processing	→	Methods that change attribute values
Storage	→	Variables for storing attributes
Dissemination	→	Get and set methods, constructors
Use of appropriate information handling methods only (Controls)	→	Encapsulation

As discussed earlier, the information contained in an object, as well as the methods used to manipulate the information, are strictly defined in the object's class definition. In addition to this, encapsulation ensures that only the appropriate, predefined, methods are used to manipulate the information. Viewing departments as objects therefore requires that: 1) all information in a department must be defined and, 2) all methods used for manipulating the information in the department must be defined. Since our model is only concerned with information privacy, this requirement applies only to private information and the methods used to manipulate private information.

The definition of all private information and related methods is the first step in the protection of information privacy. This is because it is impossible to protect information if one does not know it exists, or, if one does not know where or how it is stored and used. Once all private information and related methods in a department are defined, controls may be used to protect the information. Eloff and von Solms [18] define *controls* as measured steps taken to achieve a specific objective. In our case, the objective is to limit breaches of information privacy. Their definition, however, is not detailed enough for our purposes. Hence, we adapt the definition in the COBIT framework [19] to define *information privacy controls* (IPCs) as the policies, procedures and practices designed to provide reasonable assurance that information privacy breaches will be prevented, or detected and corrected. IPCs correspond to encapsulation in the OOP paradigm.

3.3 The OECD Guidelines

The OECD guidelines contain a set of principles referred to as the Fair Information Principles (FIPs). The FIPs provide guidance on the ethical handling of private information. The FIPs were first published in 1973 in a report by the United States Department of Health, Education, and Welfare [20]. Only four principles were listed, but these have since been developed to eight in the OECD guidelines. Globally, information privacy law is based on the FIPs [7, 8]. Due to space restrictions, we do not elaborate on the principles. For the same reason we do not list them here as they are listed in our model.

4 CONCEPTUAL MODEL

In this section we present our conceptual model. We describe each of the four elements in the model. These are: attributes, methods, controls and relationships. We then describe the interrelation between the elements in Figure 1 and show the full specification for the model in Figure 2.

4.1 Attributes

Our model is based on the object analogy. As such, we view a department as an object. The private information used by a department is represented by attributes. Attributes are classified as *electronic* if they are stored in electronic form or manual if they are stored manually (e.g. on paper). In addition, attributes may be classified as *abstract* if they refer to entities which information pertains to. For example, a paper curriculum vitae (CV) would be defined as manual attribute. The job applicant to whom the CV belonged would be defined as an abstract attribute. This is because the job applicant himself is not stored by the department.

4.2 Methods

The different tasks related to private information in a department are represented by methods. In Solove's Taxonomy of Privacy [21], tasks belong to one of the following three categories: 1) information collection, 2) information processing and 3, information dissemination. We use this notion to classify all methods in the model as *input*, *processing*, or *output* methods. Input methods indicate how information enters a department, while output methods represent how information is passed from a department to outside entities. The term 'outside entities' may refer to another department in the same organisation, or it may refer to another organisation or individual. Processing methods represent the different ways in which the information can be used by a department. Since methods relate to information, each method is related to an attribute in the model. All methods are classified as either manual or electronic.

4.3 Controls

To ensure that there is a reasonable chance that methods do not result in an information privacy breach, we introduce the *controls* element to the model. IPCs are specified here for each method. Each of the IPCs protects one or more of the FIPs in the OECD guidelines. Input, processing and output methods each have a subset of the FIPs associated with them. For example, input methods must have controls for the following FIPs: Openness, Collection Limitation, Purpose Specification, Data Quality, Security and Accountability. By ensuring that controls enforce the FIPs, the model protects organisations against IPR.

4.4 Relationships

The final element of the model is *relationships*. The relationships element describes the flow of private information between the department and outside entities. The information flow consists of the name of the outside entity and a description of the information being transferred. Information is represented by attributes, therefore attributes are included in the description of a relationship. However, sometimes only specific pieces of information in an attribute may be transferred to or from an outside entity. For example, take the case of an organisation that outsources its customer service function to an outside entity. It may only send the entity a list containing customer names and telephone numbers rather than the complete customer record for each customer. In the model we call these specific pieces of information *attribute primitives*. In the previous example, a name and telephone number are considered attribute primitives. Attribute primitives are specified in the model using capital letters and quotes to differentiate them from ordinary attributes. Thus, the attribute primitives for a name would be specified as "NAME".

The interrelation between the different elements is shown in Figure 1. Each element is represented by a block in the diagram. The block for the controls element interfaces with IPR. It is placed at the interface to signify that its purpose is to protect the attributes and methods from IPR. The attributes block is contained within the methods block to indicate that attributes should only be accessible via methods. Although there is only a single relationship element in the model, there are two blocks for relationships in Figure 1. This is to make provision for input and output relationships between multiple outside entities. Remember that outside entities may be other departments within the same organisation, or they may be other organisations or individuals.

The full specification of the model is shown in detail in Figure 2. The figure is based on a Unified Modelling Language (UML) class diagram. It differs because the 'operations' section of a UML class diagram is called 'methods' in our model. It also has additional sections for controls and relationships. To use the model in a department, one would define specifications for the attributes, methods, controls and relationship in the department. The specifications must follow the format dictated in Figure 2. A strict format is used to allow for easy parsing for implementation on a computer system. In the model specification in Figure 2, the '|' symbol is used to denote the Boolean OR function and the '+' symbol is used to denote the Boolean AND function.

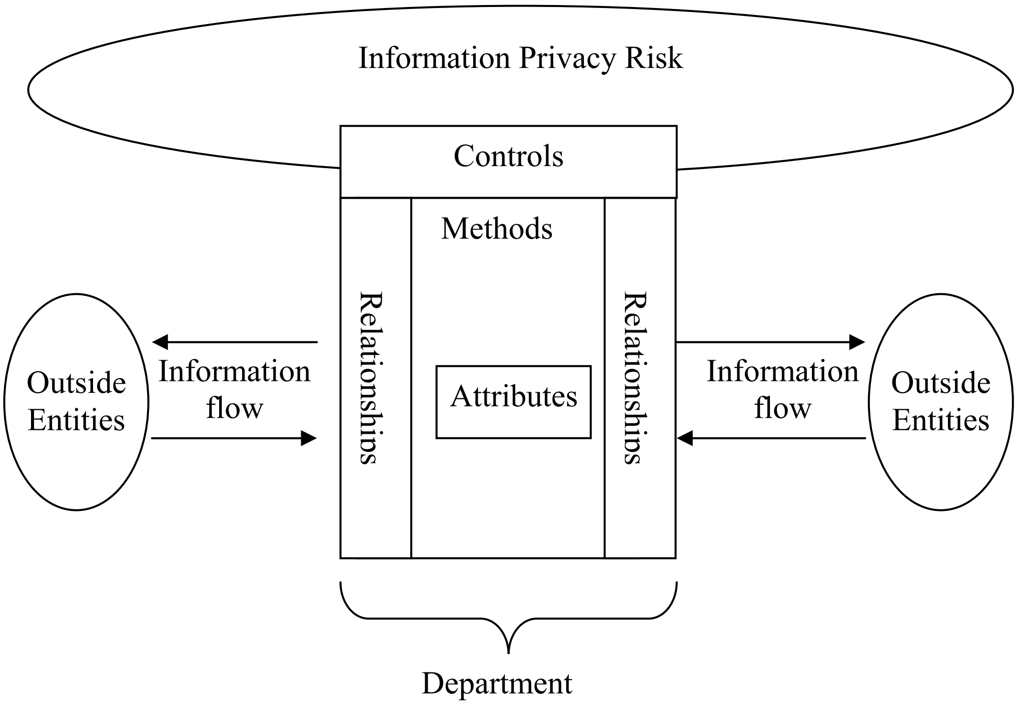

Figure 1 – Interrelation between the Elements in the Model

Figure 2 – Specification of the Conceptual Model for a specific department

Attributes

All private information held by the department is listed here in the form <attribute name_[E|M|A] : *description*> where:

E denotes an electronic copy of the information

M denotes a manual/hardcopy copy of the information

A denotes an abstract entity type to which information pertains, e.g. employee

Methods

All methods for inputting, processing and outputting private information are listed here in the form < [I|O|P]_method name_attribute name_[E|M] : *description* > where:

I denotes an input method or means used to receive private information

O denotes an output method or means used to disseminate private information

P denotes a processing method or means used to process or store private information

E denotes an electronic method

M denotes a manual method

Relationships

All relationships with outside parties are listed here in the form < [I|O]_entity name_[F|T]_{comma delimited list of attributes and/or attribute primitives} : *description* > or starting with [I+O], where :

I denotes an input relationship where private information is received from the named entity

O denotes an output relationship where private information is disseminated to the entity

F denotes another department within the organisation

T denotes a third party (another organisation or individual)

Use of the '+'operator indicates that an input and output relationship exists with the entity.

Controls

All IPCs used for each method above are listed here as < [O|CL|PS|UL|DQ|IP|S|A]_control name - method name : *description*> or starting with [O+CL+PS+UL+DQ+IP+SA], where the letters O,CL,PS,UL,DQ,IP,S,A correspond to the FIP the control is addressing.

Use of the AND operator '+' indicates that more than one principle is being addressed by the control. The FIPs are: O – Openness, CL – Collection Limitation, PS – Purpose Specification, UL – Use Limitation, DQ – Data Quality, IP – Individual Participation, S – Security, A – Accountability

Input methods must have controls that ensure the following: CL, PS, DQ, {S, A,O}[*]

Output methods must have controls that ensure the following: UL, DQ, IP, S, A, {O}[*]

Processing methods must have controls that ensure the following: UL, DQ, IP, S, A, {O}[*]

[*] FIPs in curly brackets are optional since it may not always be practical to consider them for each control

5 EXAMPLE SCENARIO

In this section we provide a practical scenario which makes use of our conceptual model. We assume the existence of a privacy management system based on our model. We make this assumption because our model is conceptual – in order to be implemented practically, a means is required to record the specifications of attributes, methods, controls and relationships.

In this scenario we consider a job applicant, Bob. Bob wishes to work at company X. In order to work at company X Bob must undergo a psychometric test[1]. The test is performed by a psychologist who requires Bob's permission to give the results to company X for the sole purpose of his job application. Bob grants his permission by signing a permission form, which is faxed by company X's human resources (HR) department. He then undergoes the test, which is performed at the psychologist's rooms. The results are emailed to the company X's HR department. The results reveal that Bob has a personality type that is easily stressed. Since Bob's job does not involve a high degree of stress he is given the job.

As an employee of company X Bob is eligible for medical aid or health insurance. It is the policy of company X, and part of Bob's employment contract, that company X pay a fixed amount towards his health insurance. It is also part of Bob's employment contract that he must insure his health through company H. This is due to the fact that company X has negotiated preferential rates with company H. Bob duly applies for health insurance from company H. In evaluating Bob's application, company H requests the results of Bob's psychometric test, since they know it is company X's policy to have psychometric tests performed on job applicants. The request is made directly to the HR department without Bob's knowledge. From the results of the psychometric test company H discovers Bob has a personality type that is easily stressed. Accordingly, they increase the premiums he must pay for his health insurance. They do this because they argue that a person who is stressed easily is more susceptible to stress-related illnesses. Bob sees that his insurance premiums are more than the standard rate and enquires about the reason. Company H

[1] This is a test based on psychometric theory. Such tests are usually designed to determine personality characteristics, aptitude, intelligence, and other psychological traits.

informs him of the reason. Bob then asks company H how they acquired the information about him. Company H notifies him and he sues his employer for breaching his privacy. Specifically, for using his information for a purpose he had not agreed to.

We now show how the model could have been used by company X to avoid such a situation. Due to space restrictions we do not define all attributes, methods, controls and relationships. We only include those necessary to protect psychometric test results and those relevant to providing a better understanding of the model. All definitions are from the point of view of company X's HR department.

We start by defining attributes for the psychometric test results (note that numbering attribute definitions is not required by the model but we do this for referencing purposes):

(1) Applicant PsychTestPermForm_M : *Manual document containing applicant's permission to use psychometric test results for health insurance*

(2) Applicant PsychTest_E : *E-mail copy of a job applicant's psychometric test results*

(3) Applicant PsychTest_M : *Manual document containing applicant's psychometric test results*

We define two attributes (2 and 3) for the test results since the test results are sometimes printed and stored in a manual file. In (2) we see the definition for the email received from the psychologist and in (3) we see the definition for the manual printout. Note the '_E' and '_M', as well as the descriptions, are used to differentiate the two. In (1) we also define the form that an applicant must sign to grant company X permission to give the results of the test to company H.

We now specify the methods related to these attributes:

(4) I_Receive Applicant PsychTest_E_E : *Receive applicant psychometric test results by e-mail*

(5) P_Print and Store Applicant PsychTest_E_M : *Print and store applicant psychometric test results in manual file*

(6) O_Send PsychTest_E : *E-mail applicant permission form to company H*

In (4) we define an input method for the receipt of the test result email defined in (2). The '_E' again specifies that this method is electronic. In (4) the processing method for printing out the email from (3) is defined. This results in the creation of the manual test results defined in (5). The fact that the email is stored in a manual file is noted by the '_M' in (4). The output method for e-mailing the permission form is also defined in (6).

We now define a control related to these methods:

(8) UL_Signed Applicant PsychTestPermForm_M - O_Send PsychTest_E: *Have applicant sign permission form for the purpose of giving test results to company H.*

The single control in (8) protects the Use Limitation principle in the OECD guidelines. This can be seen by the 'UL_' at the beginning of the definition. The Use Limitation principle states that personal information should not be made available for uses other than those specified at the time of collection. In our scenario we recall that Bob agreed to provide company X with the results of his psychometric test for the sole purpose of his job application. The control defined in (8) states that a signed permission form is required before Bob's test results may be sent via email as defined in (6). This control is sufficient to limit the risk of company X giving company H Bob's test results without his consent. If Bob does not want company H to have the results of his test, he need not sign the permission form. Thus, the likelihood of a situation such as the one in our scenario is significantly diminished.

Additional controls may also be defined to further protect Bob's psychometric test results. For example:

(9) S_Lock Applicant Files Cabinet_M - P_Print and Store Applicant PsychTest_E_M : *Lock manual files used to store applicant test results in a filing cabinet*

This control protects the Security principle in the OECD guidelines. The Security principle states that personal information should be protected by reasonable safeguards to against its loss, unauthorised access, destruction, use, modification or disclosure [6].

The relationship between company X's HR department and company H, which is the subject of our scenario can, be defined by the following:

(10) O_Company H_T_{Applicant PsychTest_E} : *E-mailing of applicant psychometric test results to company H*

The ‘O_’ at the beginning of the definition indicates that it is an output relationship. In other words, information is being disseminated from the HR department. ‘Company H’ is the name of the entity the relationship is with. The ‘T_’ specifies that the relationship is with a third party, that is, with another organisation or individual. ‘Applicant PsychTest_E’ is the name of the attribute being disseminated in the output relationship – see (2) for the definition of this attribute. The HR department’s name is not included in this definition. This is because all the definitions in our scenario up to this point are from the HR department. All relationships are therefore defined with respect to the HR department. A corresponding relationship definition from the appropriate department in company H will look like this:

(11) I_Company X HR Dept_T_{Applicant PsychTest_E}

The only difference in this case is that (11) is an input relationship since the test results are received from company X’s HR department.

6 DISCUSSION

In this section we undertake a general discussion of the conceptual model. We provide further rationale for our choice of the elements that make up the model, namely attributes, methods, controls and relationships. Furthermore, we discuss some potential uses for the model.

In order to use the model, an organisation must define the attributes, methods, relationships and controls as required by the model. Ideally, this must be done for each department that deals with private information. As mentioned earlier, the definition of attributes and methods is the first step to protecting information privacy. This is because organisations cannot protect information if they do not know it exists, or, if they do not know where or how it is stored and used. The model is holistic in that attributes may be either electronic or manual. This is important since private information exists in both forms in large organisations.

Defining attributes and methods only maps out what needs to be protected to reduce IPR. It does not specify the means by which protection will be achieved. The purpose of the controls element of the model is to specify such means. It does this by ensuring that organisations have controls in place to protect each of the FIPs. Since the model is a high-level, conceptual model, it does not dictate what these controls should be. The choice of control is left up to the organisation (e.g. role-based access control or policy based controls such as Karjoth and Schunter [10] may be used as technical controls). Knowledge of the FIPs is thus required in order to implement the model. We do not believe this is a problem for two reasons. Firstly, the FIPs are freely available [6]. Secondly, we believe the FIPs are sufficiently straightforward to understand, especially given the expertise available in large organisations. While the model does not dictate the use of specific controls, it does show which FIPs controls should protect for input, processing and output methods. Organisations are thus able to determine if controls are missing for the various aspects of information privacy defined in the FIPs. This is important because where FIPs are not protected, this results in increased IPR.

Information flow refers to the movement of attributes from one entity to another. It is an important aspect of information privacy. Inappropriate information flows can result in breaches of information privacy [22]. The control of information flows is therefore important in reducing IPR. In our model information can flow in and out of a department only via input and output methods. As discussed, controls protect the privacy of information 'flowing' through these methods. The relationships element of our model explicitly defines the relationships between a department and outside entities. This is done because the 'level of granularity' of our model is the department. That is, our model describes only a single department at a time. The relationships element thus provides a mechanism to link multiple departments by the flow of attributes between them. In other words, it allows an organisation to map inter-departmental flows of private information. It also allows organisations to map the information flows between themselves and other organisations and individuals.

It is important to note that the effectiveness of the model is dependant on accurate and complete information regarding attributes, methods, controls, and relationships. Regular updating of the model is therefore necessary because it is possible that methods, attributes, controls and relationships will change over time. The likelihood of such changes should determine the frequency with which the model is updated.

It is also important to note that the model is a high-level, conceptual management model. Its purpose is to provide guidance about the management of IPR and not to dictate specific controls or methods. Due to the structure of the model, it is easy to record the specifications for attributes, methods, controls and relationships electronically. This may be done using object or relational databases. Once recorded, application systems can be designed to interface with the databases for the purpose of managing and maintaining the model, for example, to add new controls or methods. An application system may also enforce the model's rules. An example of this would include warning a user that controls enforcing certain FIPs are missing with respect to a given method. Information flows can easily be determined with an application system by interrogating the relationships element of each department in the database. From this it will be possible to construct visual maps of information flows. An application system based on the model would, in essence, be a privacy management application. As such, it would primarily be of use to those responsible for the management of IPR. In large organisations, this may be a chief privacy officer, chief information officer or the internal audit head. Due to the rigorous specification of methods and controls, the model may also be used as the basis for privacy audit systems.

A standardisation of the model may allow for a uniform way of representing the private information in an organisation, the processing and protection thereof, as well the information flow both within and between organisations. A standard means to represent private information and its processing, protection and flow is useful in the privacy audit domain. This is because a privacy audit of an organisation will require knowledge of the private information in an organisation as well the controls employed to protect information privacy. In certain countries larger scale audits, or investigations, are carried out by privacy commissions [2]. In these countries privacy commissions are usually statutory bodies charged with protecting information privacy. If a standard means exists to represent private information and its processing, protection and flow, this will make investigations by commissions easier. The reason for this is that commissions can use applications to automatically interrogate information made available from the privacy management systems of large organisations.

7 CONCLUSION

In this paper we have addressed the need for large organisations to manage information privacy appropriately. We have done so by presenting a high-level, conceptual model for the management of IPR. The model is based on the similarity between departments in organisations and objects in object-oriented programming languages. We have provided a detailed specification of the model and discussed the various elements it is comprised of. In order to demonstrate its practical significance, we have also presented a scenario in which the model is used.

Future work on the model may include adding a 'personnel' element to the model. This element will explicitly define the roles and responsibilities of individuals within a department with regard to preventing IPR. Research will be required to determine how this element will link with the original elements in the model and what, if any, modifications to the original elements are necessary.

Further research is also needed in the practical implementation of the model. Such research may be achieved through a case study in which the model is applied to departments in a real organisation. To fully understand the potential benefits and pitfalls of a practical implementation in a real organisation, it will be necessary to develop and deploy a prototype privacy management application system based on the model.

8 REFERENCES

1. A. Daniel Oliver-Lalana, “Consent as a Threat. A Critical Approach to Privacy Negotiation in e-Commerce Practices”, In: *TrustBus 2004*, *LNCS,* Vol. 3184, S. Katsikas., J. Lopez, G. Pernel (eds.), pp. 110-119, Springer, Heidelberg, 2004

2. *Discussion Paper 109, Project 124, Privacy and Data Protection*, South African Law Reform Commission, Pretoria, 2005

3. R. Clarke, “Introduction to Dataveillance and Information Privacy, and Definitions of Terms”, Department of Computer Science, Australian National University, 2006. Available: http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html

4. A. Ghobadian and D. Gallear, "TQM and organization size", *International Journal of Operations & Production Management*, Vol. 17, No. 2, pp.121-63, 1997

5. S.E. Chang and C.B. Ho, “Organizational factors to the effectiveness of implementing information security management”, *Industrial Management & Data Systems*, Vol. 106, No. 3, pp. 345-361, 2006

6. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Organization for Economic Cooperation and Development, Paris, France, 1980. Available at: http://www.oecd.org/document/57/0,3343,en_2649_201185_1815186_1_1_1_1,00.html

7. C.S. Powers, P. Ashley, M. Schunter, “Privacy Promises, Access Control, Privacy Management”, In: *Proceedings of the 3rd International Symposium on Electronic Commerce*, North Carolina, USA, 2002.

8. R. Gellman, “Does Privacy Law Work?”, In: *Technology and Privacy: The New Landscape*, P.B. Agre and M Rotenberg (eds), pp. 194, The MIT Press, 1998

9. R. Purcell, “Privacy by 3PT®: A Management Model”, *Corporate Privacy Group*, Nordland, Washington, USA. Available: http://www.corporateprivacygroup.com/CPG_3PTMGMTMODEL.pdf

10. G. Karjoth and M. Schunter, “A Privacy Policy Model for Enterprises”, In: *Proceedings of the 15th IEEE workshop on Computer Security Foundations*, Nova Scotia, Canada, pp. 271, 2002

11. P. Ashley, S. Hada, G. Karjoth, C. Powers, M. Schunter, “Enterprise Privacy Authorization Language (EPAL 1.2)”, *International Business Machines Corporation*, 2003. Available: http://www.zurich.ibm.com/security/enterprise-privacy/epal/Specification/

12. M. Casassa Mont, “Dealing with Privacy Obligations: Important Aspects and Technical Approaches”, In: *TrustBus 2004*, *LNCS,* Vol. 3184, S. Katsikas., J. Lopez, G. Pernel (eds.), pp. 120-131, Springer, Heidelberg, 2004

13. M. Casassa Mont, “Towards Scalable Management of Privacy Obligations in Enterprises”, In: *TrustBus 2006*, *LNCS,* Vol. 4083, S. Fischer-Hübner et al. (eds.), pp. 1-10, Springer, Heidelberg, 2006

14. J. Biskup and H.H. Brüggemann, “The Personal Model of Data: Towards a Privacy-Oriented Information System”, *Computers & Security*, Vol. 7, No. 6, pp. 575-597, 1988

15. J. Biskup and H.H. Brüggemann, “The Personal Model of Data Towards a Privacy-Oriented Information System”, In: *Proceedings of the Fifth International Conference on Data Engineering*, California, USA, 1989

16. D.J. Armstrong, “The Quarks of Object-Oriented Development”, *Communications of the ACM*, Vol. 49, No. 2, 2006

17. L.F. Capretz, “A Brief History of the Object-Oriented Approach”, *ACM SIGSOFT Software Engineering Notes*, Vol. 28, No. 2, 2003

18. M.M. Eloff and S.H. von Solms, “Information Security Management: A Hierarchical Framework for Various Approaches”, *Computers & Security*, Vol. 19, No. 3, pp. 243-256, 2000

19. *COBIT 4.0*, IT Governance Institute, pp. 14, Rolling Meadows, Illinois, 2005. Available:
http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=27263

20. *Privacy Online: Fair Information Practices in the Electronic Marketplace – A Report to Congress*, Federal Trade Commission, pp. 3-4, Washington D.C, USA, 2000. Available at http://www.ftc.gov/reports/privacy2000/ privacy2000.pdf

21. D.J. Solove, “A Taxonomy of Privacy”, *University of Pennsylvania Law Review*, Vol. 154, No. 3, 2006

22. L.C.J. Dreyer and M.S. Olivier, “An information flow model for privacy (InfoPriv)”, In: *Database Security XII: Status and Prospects*, S. Jajodia (ed), pp. 77–90, Kluwer Academic Publishers, 1999