Eurasian Journal of Business and Management, 1(1), 2013, 15-31

EURASIAN JOURNAL OF BUSINESS AND MANAGEMENT

http://www.econjournals.net

BUILDING A PRIVACY MODEL IN THE BUSINESS PROCESSES OF THE ENTERPRISE: AN INFORMATION SYSTEMS DESIGN SCIENCE RESEARCH

Munir Majdalawieh[1]
Zayed University, U.A.E. Email: Munir.majdalawieh@zu.ac.ae

Abstract

Privacy has not been researched or investigated from business process management perspective and the current literature has shown lack of a well-defined methodology for integrating privacy into business processes. This paper proposes an integrated privacy model. Such model is an integral part of the organization's enterprise to ensure that personal data protection is impeded in the business processes of any system that is involved in collecting, disseminating, and accessing an individual's data. Passing privacy laws is very essential and requires some cooperation and partnership between nations based on some privacy principles. The proposed framework is built on these principles and will help organizations to develop data protection in their business processes, assess the privacy issues in their organization, protect the interest of their clients, advance their value proposition, and make it easier to identify the impact of privacy on their business. The study follows the design science research process and the information systems design science research (ISDSR) methodologies by identifying relevant problems from the current literature, defining the objectives of the study, designing and developing the ABC-PDMS model, and evaluating the model.

Keywords: Privacy, Protection, Data, Information, Framework, ERP, Business Processes, Legislation, Law, ABC-PDMS, Design Science Research Process, Information Systems Design Science Research (ISDSR)

[1] Dr. Munir Majdalawieh is an academic researcher and a practicing Enterprise Information Systems professional. He is on the IS faculty of Zayed University, Dubai, UAE and the coordinator of the Enterprise Computing program. He has a Doctorate in Information Technology and EMBA from George Mason University, USA and a M. Sc. from Northeastern University, USA. He has written about internal auditing and control, IT security and privacy, risk management, corporate and IT governance, business process management, strategic changes in IT/IS technologies and management in academic and practitioners' refereed journals and conference proceedings. Dr. Majdalawieh previously worked for the American University of Sharjah in UAE for six years and worked for Booz Allen Hamilton, Hewlett Packard, Compaq Computer Corporation, and Digital Equipment Corporation in the United States for more than 22 years. Dr. Majdalawieh is an active member of the IIA, ISACA, and RIMS.

1. Introduction

In the digital and Internet "DigNet" age, organizations are utilizing the Internet by interacting with their suppliers, customers/clients or citizens (clients) and in most cases they collect and use the personal data for a variety of purposes. When sensitive personal data are being processed, extra controls must be applied. How to protect privacy rights in the "DigNet" age has been a recurring problem since the inception of the Internet. Clarkson *et al.* (2009) indicate that individuals in the "DigNet" age are not aware that information about their personal lives and preferences is being collected by Internet companies and other online users without even getting the permission to do so. Because of these concerns and the possibility of lawsuits based on privacy laws, online businesses post on their web sites a privacy policy statement (PPS) disclosing how personal data obtained from their online users will be used and to provide the users with some assurance about how the organization will protect and use their personal data. While the vast majority of online users claim they are concerned about their privacy, less than 50% have read the PPCs on Web sites (Laudon and Traver, 2008).

The amount of interest and research on privacy testifies to its relevance. Researchers and practitioners through empirical and field studies indicate that online users are skeptical when it comes to privacy and the Internet in general and online business in specific. The impact of privacy on online businesses is very significant. Teifke (2003) believes the impact of the potential loss of privacy takes on a whole new meaning when we look at the issue from the perspective of our individual companies. A 2005 poll conducted by Web Design Directory (2005) indicated that 62% of the 1000 adults surveyed are worried their personal data could be stolen online. A joint study by TNS and TRUSTe (2008) found that lack of transparency may factor into privacy concerns that online users have. Among the 1,015 interviewers, 71% of the participants are aware that their browsing information may be collected by a third party for advertising purposes. The percent did not change much for the same survey in 2009 (TNS and TRUSTe). This indicates that the online users are aware of the privacy issues and the challenges they are facing when conducting business or just browsing on the Internet. As such many online businesses are missing huge amount of growth because they are not giving enough assurance to the users that their personal data is protected.

Pirim *et al.* (2008) argue that privacy has been empirically studied in the information technology research from an organizational context. They added that from a general individual perspective privacy has not been addressed in relation to Information Technology. Furthermore, privacy has not been researched or investigated from business process management perspective (FTC, 2010) and the current literature has shown lack of a well-defined methodology for integrating security and privacy into business processes (Anderson and Rachamadugu, 2008).

The proposed advanced business-centric personal data management system (ABC-PDMS) conceptual model is built on predefined principles and will help organizations to integrate privacy in their business processes. Furthermore, the system will give clients more control on the usage of their data and give organizations more control to fulfill the compliance requirements from their own policies and the government's legislations.

2. Methodology

To ensure ABC-PDMS's rigor, we draw upon the design science research process (Peffers *et al.* 2008) and the information systems design science research methodologies (Hevner *et al.* 2004) and define their steps in the context of this study:

2.1. Problem Identification and Motivation (Relevance Cycle)

The background section of the paper reviews the literature to understand the state of the problems that motivate the need for and drive the development of ABC-PDMS model. Summarizing, the three main problems identified are (a) no established privacy conceptual model has been developed as of yet (Anderson and Rachamadugu, 2008); (b) privacy has not been addressed in relation to Information Technology (Pirim *et al.* 2008); and (c) existing Privacy frameworks lack a well-defined methodology for integrating privacy into the business processes of the enterprise (Anderson and Rachamadugu 2008; FTC, 2010).

2.2. Objectives of the Solution (Implicit in "relevance")

Based on the aforementioned problems, we identify three main objectives of this study: (***obj1***) build an advanced business-centric personal data management system (ABC-PDMS) based on predefined principles; (***obj2***) facilitate the integration between personal data management system and business information processing within an enterprise using different building blocks; and (***obj3)*** give organizations insight into how the proposed framework help organizations to develop data protection in their business processes and to enhance their performance.

2.3. Design and Development (Iterative Search Process)

In order to explicate the design of the solution that fulfills the objectives, we first carried out an extensive review of related literature (BACKGROUND section) which proposed that currently no sufficient data protection conceptual framework solution exists. Hence, ABC-PDMS was proposed through several iterations to ensure that we have a complete and sound solution. To address (***obj1***) we identified the building blocks of the ABC-PDMS in light of the three key domains: 1) the data protection legislation, 2) the data protection policies and procedures, and 3) the data protection controls and the associated privacy services. To address (***obj2***) we: (i) introduced the ABC-PDMS five Processes; and (ii) extended this set of elements to address requirements that come from Service-Oriented Architecture (SOA) principles by introducing privacy services as part of the proposed model. To address (***obj3***) we demonstrated how to integrate the ABC-PDMS into the business processes of the enterprise by using the order-to-cash (O2C) as an example.

2.4. Evaluation (Evaluate)

Preliminary evaluation regarding the validity, the usability, the adaptability and the usefulness of ABC-PDMS are discussed. We evaluate the model in terms of the objectives of our study. We used the O2C business process to illustrate our solution (Integrating ABC-PDMS in the Order-to-Cash (O2C) business process section), trusting that our proposed conceptual model will add value to the privacy body of knowledge of literature and practice.

3. Background

3.1. Analysis of the Current Status of Privacy

Privacy is a shared responsibility between the organization that is processing the personal data, the individual who is providing the data, and the government in which the organization is operating. The government responsibility is to issue and to enforce data protection legislation. Recently there has been an increased concern over the status of data protection laws in specific

countries. But the issue is beyond the boundaries of a specific country. The data could be collected in one country, accessed from another country, and yet distributed to other countries. It is the responsibility of the organization to establish policies and procedures related to data privacy and to provide control mechanisms to ensure that these policies and procedures are maintained. Controls should be established to ensure that the data is accurate and secure when it is in processing (DIP), in transmission (DIT), and at rest (DAR). The individual's responsibility is somewhat limited to provide his/her data to a legitimate organization and to use Internet tools to protect his/her data and privacy (EPIC) when is possible.

Privacy means different things to different people. The definitions of privacy vary widely according to concept, context and environment. In general, privacy means the right to an individual to be left alone and the right to be free of unreasonable personal intrusion by government, individuals, or organizations. Privacy concerns exist way before the "DigNet" age. Westin (1967, p.7) defined privacy as "the individual's right to determine or control the distribution of their information, including how it is collected, used and distributed, to whom it is provided, and to what extent it is released." The principles of this definition are essential components of our proposed framework.

The concept of data protection has been fused with privacy, which interprets privacy in terms of personal information management. Privacy can be divided into four separate but related concepts: physical or bodily privacy, territorial privacy; privacy of communications, and information privacy/data privacy. The focus in this paper is on the privacy of information and communications. Privacy of information involves the establishment of rules governing the (DIP), (DIT), and the (DAR) of personal data. Privacy of communication covers the security and privacy of retrieving data from databases through applications within the enterprise or outside the enterprise such as e-mail and other forms of communication.

The increase in privacy concerns in the "DigNet" is well documented (Majdalawieh 2010; Lwin *et al.* 2007; Ashworth and Free 2006; Peslak 2005a, 2005b, 2006, and 2007; Milne 2000; Thomas and Maurer 1997). Such concern is shared among individuals, organizations, and governments. The growing capabilities in the "DigNet" are making it easier to collect, share, transmit, sort, file, access, and convert data to information and in turn convert it to knowledge. Such capabilities forced individuals, organizations, and governments to study a balance between privacy and participation (Westin, 1967). Individuals would like to participate in the "DigNet" activities, but they are very concern about their privacy and how organizations and governments are handling the processing of their information. Organizations would like to have more users to participate in the "DigNet" activities to increase their sales of products and services and to collect accurate personal data to be used in the development of databases. The databases will be used for future marketing and sales decisions and campaigns. To accomplish this goal, they are working very hard to provide individuals with some assurances about the protection of their data and privacy. The lack of solutions for the protection of personal data and the way organizations are collecting and using such data is very important and relevant to the study of privacy. Relevance as one main cycle of the design science methodology is well defined in our privacy solution. The application domain is represented by the people (individuals) and organizational (organizations, government) as the main environmental component of the input requirements.

The focus so far for practitioners and researchers in addressing the issue of privacy is in protecting personal data, providing tools for end users to manage their data (IPEC), providing a privacy policy statement, and satisfying the raw requirements imposed by the government's privacy laws.

3.2. Understanding Proposed Models for Privacy

Serwin (2010) discussed three main proposed models for privacy: Accountability (Feigenbaum, 2010), Processing Limitations, and Proportionality. An accountability model generally focuses on after the fact enforcement. Processing limitations (use-based restrictions) model focuses on receiving consent of individuals or by the authority of law to disclose or make the personal data available. Use-limitations model should be proportional to the sensitivity of data.

Accountability should not be the focal point of privacy theory, particularly since the experience proves the model has not worked (Serwin, 2010). Processing limitation should be used as part of a whole privacy system within a framework of defining what kind of data we need to restrict or what individuals are asking us to restrict. Use-limitations should be proportional to the sensitivity of data based on four tiers classification—highly sensitive; sensitive; slightly sensitive; and non-sensitive (Serwin, 2010). Such limitation is appropriate but it should be part of a whole privacy model to deal with how it is integrated in the enterprise.

In recent years, the FTC (2010) has sought to advance this objective using two primary models: the “notice-and-choice model,” which encourages companies to develop privacy notices describing their information collection and use practices to consumers, so that consumers can make informed choices, and the “harm-based model,” which focuses on protecting consumers from specific harms – physical security, economic injury, and unwanted intrusions into their daily lives. Each model has significantly advanced the goal of protecting consumer privacy; at the same time, each has been subject to certain criticisms.

The Federal Trade Commission (FTC, 2010) recently issued report, "Protecting Consumer Privacy in an Era of Rapid Change: A proposed Framework for Businesses and Policymakers". The report proposes a framework with three principles: “Privacy by Design”, “Simplified Choice”, and “Greater Transparency”. Organizations should promote consumer privacy throughout their organizations and at every stage of the development of their products and services (FTC, 2010). These privacy models have been discussed from design point of view, the discussion also should be focused on implementation of these models (Serwin, 2010). This paper is taking into considerations the principles proposed by these models and integrate them into the proposed framework.

3.3. Privacy Protection Laws

In many countries around the world, governments established laws to protect and govern the privacy of individuals’ personal data. In most cases the government has a “privacy” agency to monitor and evaluate the private and public companies to ensure compliance with its legislations. In the United States, privacy of citizens is protected primary by the constitution in addition to many US federal and state acts that set forth the principles for handling personal information in such areas as credit reporting, financial records, education records, newspaper records, search engines records, and electronic transaction records. The Privacy Act of 1974 is considered to be the father of all privacy laws since it sets the foundation of regulating how the federal government agencies can collect, use, and disclose an individual’s data and information. The Gramm-Leach-Bliley Act of 1999 requires financial institutions to ensure the security of client data.

Many other laws including: Electronic Communications Privacy Act of 1986, Computer Matching and Privacy Protection Act of 1988, Computer Security Act of 1987, Driver’s Privacy Protection Act of 1994, and E-Government Act of 2003 established to protect the privacy of individuals (Laudon and Traver, 2008). Laudon and Traver (2008) indicate that most of the U.S. federal privacy laws apply only to the federal government and regulate very few areas of the private sector.

Based on the "Recommendation Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" issued by the Organization for Economic Cooperation and Development (OECD, 1980) the European Union (EU) has issued certain guidelines, according to which countries in EU will cease to share data considered the subject matter of protection to any third country unless they adhere to similar laws. Though there are commercial interests behind these guidelines, very few countries within the EU can stay away from these guidelines. Canada and Australia adopted several laws described as a "co-regulatory model." Under these laws, companies representing the industry develop rules for the protection of data that are enforced by the industry and overseen by a "privacy" agency. Furthermore, in January 1, 2004 the Canada's federal government's personal privacy protection legislation was enforced. This legislation is based on the Personal Information Protection and Electronic Documents Act (PIPEDA). As a result, companies started getting their "privacy" practices in order to be compliant with the law or they will face potentially damaging consequences (Williams, 2003).

In general, most of these laws established several principles in which every organization must meet the obligations declared in these principles. Failing to comply with these principles could have serious implications including: audit of the organization's privacy practices, public reports about the audit's findings, litigation in the federal courts with the prospect of fines, sanctions, and/or criminal liability, and substantial legal and privacy compliance costs.

Some of these principles include collection limitation principle, data quality principle, and purpose specification principle. These principles will be discussed in more detail later on in our paper since they are part of our framework. These principles are considered to be complete and when the United States agrees to go by these guidelines, they will be considered universal standards.

3.4. Privacy Protection Solutions

As mentioned earlier, privacy protection is the responsibility of the organization that is processing the personal data, the individual who is providing the data, and the government in which the entity is operating. In addition to legislation, several tools are available for online customers to protect their privacy when they interact with online businesses. Epic provides comprehensive privacy-enhancing tools to secure and protect privacy on the client web browser machines. Many of these tools are used for encrypting e-mail, files and folders; for preventing client machines from accepting cookies; by disabling the monitoring and recording the sites visited; and by detecting and eliminating spyware and web bug programs.

Past research in the field of privacy and the protection of personal data in the "DigNet" era produced formal and rigorous results that have been used for the design of many practical privacy solutions. As a result of these research activities, there are now tools to help users determine the kind of personal data that can be extracted by Web sites. The Platform for Privacy Preferences Project known as (P3P) enables Web sites to develop their PPCs in a standard format through an interactive Privacy Policy Editor that can be retrieved automatically and interpreted easily by user agents. P3P user agents will allow users to be informed of site practices (in both machine- and human-readable formats) and to automate decision-making based on these practices when appropriate. Thus users need not read the privacy policies at every site they visit (W3C). P3P works only between members of the WWW consortiums who have translated their privacy policy into P3P format. Furthermore P3P provides mechanisms for users to trust the web site that they are visiting, but this trust is associated with the first visit. P3P does not provide any mechanisms for users to be informed by the organization when they use their data later on.

Government agencies continuously are developing several programs and enhancing their strategy for addressing security and privacy challenges. Federal Information Security Management Act (FISMA, 2006) report reveals modest success in meeting several key privacy performance measures including: program oversight (all agencies report having a privacy official who participates in privacy compliance activities), Privacy Impact Assessments (PIAs) for applicable systems, and Systems of Records Notices (SORNs) focusing on developed, published, and maintained systems that contain personally identifiable information.

In 2006, several U.S. federal agencies reported high profile data security breaches involving Personal Identifiable Information (PII). During Clay Johnson's (OMB, 2003) testimony before the Committee on Oversight and Government Reform, she described the inter-relationship between security and privacy programs by indicating that personally identifiable information is an example of what to protect, while security is a program for how to protect it.

OMB (2003) issued policy M 07-16, "Safeguarding Against and responding to the Breach of Personally Identifiable Information," which directs federal agencies to develop and implement a risk-based breach notification policy, while ensuring proper safeguards are in place to protect the personally identifiable information. This is evidence of how even government bodies are looking at privacy only as an inter-related to security and not addressing the real problem to measure the success of integrating these policies and programs in the business processes of organizations to develop the right strategies related to privacy.

Although these solutions can be very effective to protect individual's data, they are looked at only from security and safeguard dimension. By continuing focus on security and safeguard mechanisms will shift the responsibility from management to the technical department. So, an organization will focus on the technical solutions and let go of the business and legislation requirements.

4. Design Data Protection Solution for the Enterprise

The right of individual's to determine and control the processing of their data is an issue that researchers and practitioners have been struggling in proposing and implementing. Governments to enforce organizations to be compliant by the "privacy" laws they are asking them to do combinations of the following actions: appoint a "privacy" officer, conduct a "privacy impact assessment" to determine the type of information collected, create and implement a "Privacy Policy" to govern the organization's processing of personal information, and develop training programs for employees (OMB, 2003). As such organizations must develop a practical framework to comply with the "Privacy" laws established in the countries they do business in, or the cost of business risk will be very high on these organizations.

4.1. Traditional Personal Data Management Systems

The protection of personal data to satisfy the requirements of information and communications privacy should be part of the business processes implemented in the enterprise. The business processes related to data processing implementation is the basis for the interactions between the operational, management, and information processes of the enterprise (Gelinas *et al.* 2004). These processes should work together to accomplish the goal of an enterprise organization to maintain the privacy of individual's conducting business with.

Most of the organizations today are using the traditional personal data management system (TPDMS) to claim that they are protecting the privacy of individuals. The essence of TPDMS is for the client to trust that the organization will treat his/her data with care as per its PPC. The organization's management sets the privacy policies and controls and it is responsible for monitoring and evaluating the privacy activities to ensure that they are compliant

with the government privacy legislations. A client upon ordering products or services visits the organization's Web site through the information systems process, reads the PPC, and provides personal data to fulfill the requirements of accepting the term and conditions of the organization's PPC. A client usually will be provided with a username and password to access his/her account in case s/he wants to update their data records. Beyond this, the client has no control on the processing of his/her data. In some cases the organization could decide to share the client's data with other third parties or to use the data internally for marketing or sales purposes or even worse, some employees could access the data for personal gains.

5. Advanced Business Centric Personal Data Management Systems

The proposed ABC-PDMS will give users more control on the usage of their data and give organizations more control to fulfill the compliance requirements from their own policies and the government's legislations. As part of the design phase of the design science, we went through several iterations to come up with the proposed solution. The ABC-PDMS consists of three domains, five processes, and their activities (privacy services).

5.1. ABC-PDMS Three Domains and Their Privacy Services

After the analysis detailed in the previous sections, a multiphase iterative abstraction exercise (*Hevner et al.* 2004; Hevner, 2007) was carried out, where the proposed components of the ABC-PDMS were reviewed and identified. The abstraction exercise aimed at developing ABC-PDMS model that would: (***obj1***) build an advanced business-centric personal data management system on the principle of predefined components; (***obj2***) facilitate the integration between personal data management system and business information processing within an enterprise using different building blocks; and (***obj3***) give organizations insight into how the proposed personal data management system help organizations to develop data protection in their business processes, assess the privacy issues in their organization, protect the interest of their clients, increase their value proposition to clients, and make it easier to identify the impact of privacy on their business.

Data protection in the ABC-PDMS is built on three main domains: ***data protection legislation***, ***data protection policies and procedures***, *and* ***data protection controls***. The central portion of Figure 1 demonstrates the relationship between these three domains in relationship to personal data. Each domain consists of its own principles (Privacy Services). The privacy services are routines that interact with the internal, external, and the personal data store for processing.

The ***data protection legislation domain*** is built on what has been known as the universe data privacy regulation principles (legislation privacy services) that many governments are adopting as part of their data privacy legislations. The legislation privacy services (Williams, 2003) are: Authority (**Consent**); Collection Limitation (**Limiting**); Data Quality (**Accuracy**); Purpose Specification (**Purpose**); Use Limitation (**Processing**); Security Safeguards (**Security**); Openness (**Openness**); Individual Participation (**Access**); Challenges Compliance (**Compliance**); and Accountability Principle (**Accountability**).

The ***data protection policies and procedures domain*** is built on the universe data protection principles (organization privacy services) outlined above in addition to several resources addressed this issue (Aston, 2001 and W3C, 2007). The organization privacy services include: What, Why, How, and Who (**WWWW**); Security and Safeguard (**Security**); Publicly Available Information (**Public**); Subject Consent (**Consent**); Sensitive Data (**Sensitive**); Right of Access to Data (**Access**); and Retention of Data (**Retention**).

The ***data protection controls domain*** is built on many available procedures, tools and techniques (control privacy services) to secure an individual's data. The control privacy services include: Data Collection (**Collection**); Data Accessibility (**Accessibility**); Data Dissemination (**Dissemination**); Data Accuracy (**Accuracy**); Data at Rest (**DAR**); Data in Processing (**DIP**); and Data in Transmission (**DIT**). Organizations should develop and deploy controls to protect data collection, data accessibility, data dissemination, and data accuracy. In addition controls should be established to protect data at rest, data while in processing, and data while in transmission. Controlling DIP includes: collecting data, organizing, altering, adapting, retrieving, combining, and erasing or destroying the data. Controlling DIT includes: transmitting, sharing, and disclosing the data. Controlling DAR includes: holding or keeping data on file on storage without doing anything to or with it. It is the management responsibility to ensure that these controls are sufficient to meet the government privacy legislations and to meet the organization's goals and objectives.

In ABC-PDMS, the privacy services of each domain should be integrated in every business process of the enterprise. Such integration guarantees that the organization is providing a client with a clear PPC in which it is linked to the data protection legislation, the data protection policies and procedures, and the data protection controls. In such, the data protection legislation principles are covered in the policies and procedures of the enterprise and the data protection controls are a manifestation of both the data protection legislation and the data protection policies and procedures (See Figure 1). Moreover the client will have complete control when s/he submits his/her data, updating the data, or anytime the host organization is attempting to use the data internally or externally.

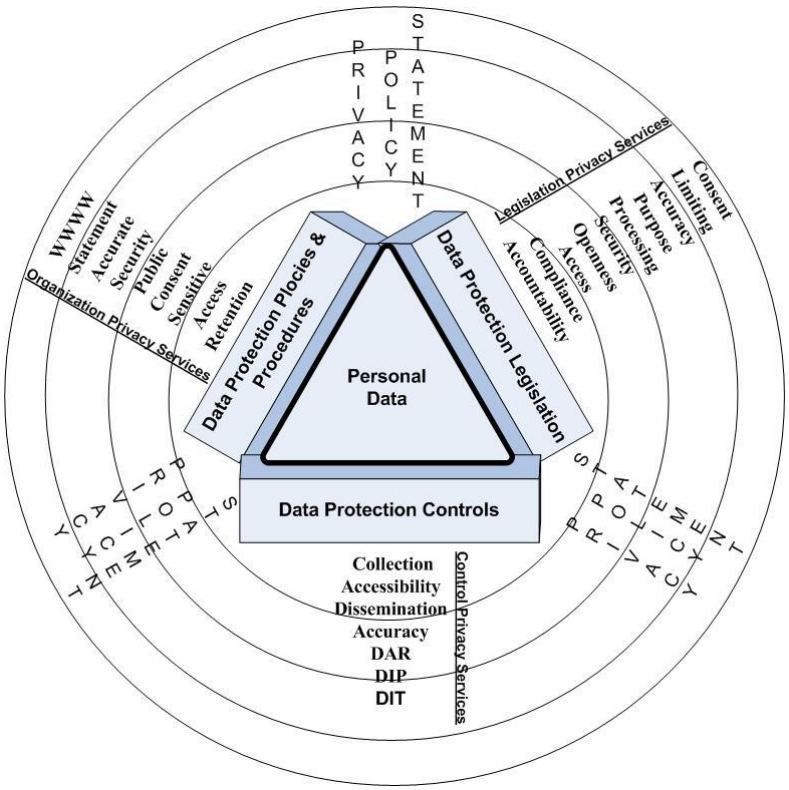

Figure 1. The privacy services (principles) of the three domains in the ABC-PDMS

The ABC-PDMS interacts with internal processes and external entities. The main two external entities are a client or any third party requests data about a client record. In the ABC-PDMS the client is in control of his/her data through any activity the organization is conducting using his/her data. The organization must receive an approval from the client anytime access to his/her data is processed. ABC-PDMS shifts the control from trusting the organization that collecting and processing the personal data as they wish to practice the right of clients to determine or control the distribution of their data, including how it is collected, used and distributed, to whom it is provided, and to what extent it is released (Westin, 1967).

5.2. ABC-PDMS Five Processes

To facilitate the integration with the enterprise business processes, the ABC-PDMS consists of five main processes (represented by the bubbles as shown in Figure 2) to manage and control the processing and the flow of personal data. The five processes are: **R**eceive PPS, **C**ollect Data, **A**ccess Data, **A**ccurate Data, and **D**isseminate Data. These processes interact amongst themselves and with external entities (represented by the rectangles) at the same time. External entities are providers and recipients of data inputs and outputs to and from the ABC-PDMS respectively, which in a typical setting includes clients (data provider) and third parties (interested in accessing personal data). Such interactions are briefly described below.

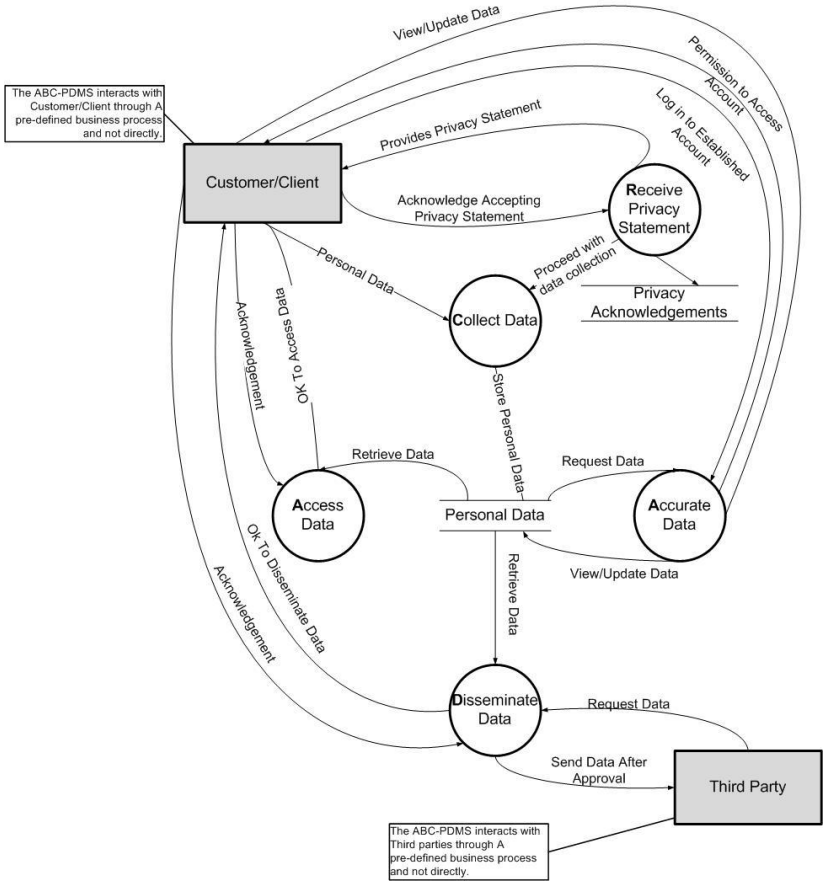

Figure 2. Logical DFD for the ABC-PDMS

As its name indicates, the ***receive* PPC process** is responsible of presenting the PPC to the client and receive the acknowledgement that s/he has read the statement and agreed upon the contents. Such acknowledgement will be recorded in a privacy acknowledgement data store. The second process is the ***collect* data process**. It is responsible for collecting the personal data from a client after receiving the acknowledgement and stores the data into the personal data store. The next process is the ***access* data process**. It is responsible for communicating with the client at any situation when any other process within the organization requests data from the personal data store. This process will ensure that an approval from the client who owns the data is obtained before the process can release the data. The next process is the ***disseminate* data process**. This process will be activated when any external entity requests data or information about individuals. The process will seek approval from the client to send the data to the external entity and will not release the data until it receives the approval. The last process is the ***accurate* data process**. It will be invoked when the client wants to access his/her data in case s/he wants to make any changes or check his/her data. In such a case s/he will be able to make any changes to the data. The organization will have some control to not allow the client to delete some data that will help in identifying him/her.

5.3. ABC-PDMS Domains/Processes and their Main Privacy Services

The five processes discussed above should be integrated with the three main domains of the ABC-PDMS. By focusing on the business processes the organization will decide starting in the initiation phase of the system development which privacy services within each domain/process required to be part of which business process. This model will give management more control on personal data activities to ensure the compliance with the government's legislation and their own policies and procedures. The PPC will be maintained and will reflect how the organization is handling data as part of the actual business processes of the enterprise. The ABC-PDMS and its five business processes, the three domains, and their privacy services are described below.

The ***receive PPC (receive) process*** is responsible for communicating with the client and receive acknowledgement that s/he has read the statement and she/he agreed on the contents of it. The receive process has consent, purpose, security, openness, and compliance legislation privacy services. These privacy services should be developed and activated for the legislation domain to ensure compliance with the government legislations' related to privacy. Similarly, the receive process has WWWW, security, consent, sensitive, and public organization privacy services. These privacy services should be developed and activated for the policies and procedures domain to ensure compliance with the organization's policies and procedures. Likewise, the receive process has DAR control privacy service. These privacy services should be developed and activated for the data controls domain to ensure compliance with the organization business strategy.

The ***collect data (collect) process*** with its privacy services is responsible for collecting the personal data from the client and store the data into the personal data store. The collect process has limitation, purpose, security, openness, and compliance legislation privacy services. Also, the collect process has WWWW, security, public, consent, sensitive, and retention organization privacy services. In addition, the collect process has collection, DAR, DIP, and DIT controls privacy services.

The ***accurate data (accurate) process*** with its privacy services is responsible for responding to a client request when s/he wants to make any changes to his/her own data. The accurate process has accuracy, security, openness, and compliance legislation privacy services. Similarly, the accurate process has accuracy, security, and retention organization privacy services. In addition, the collect process has accuracy, DAR, and DIP controls privacy services.

The ***access data (access) process*** with its privacy services is responsible for communicating with the client when any other process in the enterprise requests any personal information about the client and it should receive acknowledgement from the client before it releases any information to that process. The collect process has access, security, openness, and compliance legislation privacy services. Likewise, the collect process has WWWW, security, access, public, and retention organization privacy services. In addition, the collect process has accessibility, DAR, and DIP controls privacy services.

The ***disseminate data (disseminate) process*** with its privacy services is responsible for responding to any external entity that requests information about a client. The process will seek acknowledgement from the client before releasing any information. The disseminate process has processing, limitation, security, openness, and compliance legislation privacy services. Likewise, the disseminate process has consent, security, retention, and public organization privacy services. In addition, the disseminate process has dissemination, DAR, DIP, and DIT controls privacy services.

6. Integrating ABC-PDMS in the Business Processes of the Enterprise

According to a survey of 5,000 US customers released by Gartner (2008) about 39% say they have made a change to their online shopping behavior due to worries about their personal data being stolen. The result of the survey mentioned in the report "2008 Data Breaches and Financial Crimes Scare Consumers Away," also reveals that 59% of those who have changed behavior say they have cut online shopping. Of those, 30% say they shop less online and 28% say they abandon a session if redirected to another web site to enter payment information. 71% say they are more cautious about where they purchase online, 67% more careful about entering personal and financial information on web sites and 15% say they have stopped shopping on the web completely. To regain the consumers' confidence, organizations need to change their behavior towards the management of the consumers' personal data.

New technologies based on m-commerce associated with personal digital assistants (PDAs) and Smartphones have become so popular that organizations can integrate their capabilities in more efficient method in the ABC-PDMS to reach and communicate with their clients. With such integration, the management team will ensure that the organization is compliant with legislation laws and its own policies and procedures. Moreover, the organization will develop a trust with its clients by ensuring that their personal data is protected and they have full control of the usage of their own data. As a result, such system will give the organization a very strong personal data management value proposition since it will increase clients confidence, increase the penetration rate of customers doing business with such an entity, increase client base, increase revenues, increase market share, and improve client retention levels.

The ABC-PDMS system will be the interface with the client through the organization enterprise business processes. Such integration will guarantee that one centralized business process will be responsible for such interaction. The O2C will be used as an example to validate and demonstrate how the ABC-PDMS integration in the business processes of the enterprise takes place (See Figure 3).

6.1. Integrating ABC-PDMS in the Order-to-Cash (O2C) Business Process

The Order-to-Cash (O2C) business process helps companies to measurably improve and manage their O2C end-to-end processing life cycle. The O2C spans multiple steps including: order fulfillment, shipping & delivery, invoicing & billing, and payment. According to Wipro (2008), customer experience in the O2C process is perceived through 4 key requirements:

choice, predictability, flexibility, and cost. A product/service organization needs to deliver these requirements to meet client perception. Today, most organizations are focusing on enhancing such process from operational aspects to increase the effectiveness and the efficiency of the life cycle. The main driven factors are related to direct gains in revenues and market share. The integration of the ABC-PDMS into such process will help organizations to meet these goals in addition to gain and retain new clients by satisfying them when it comes to controlling their personal data. Integrating ABC-PDMS into the O2C process will be established by introducing three phases of O2C: Pre-O2C, O2C, and Post-O2C.

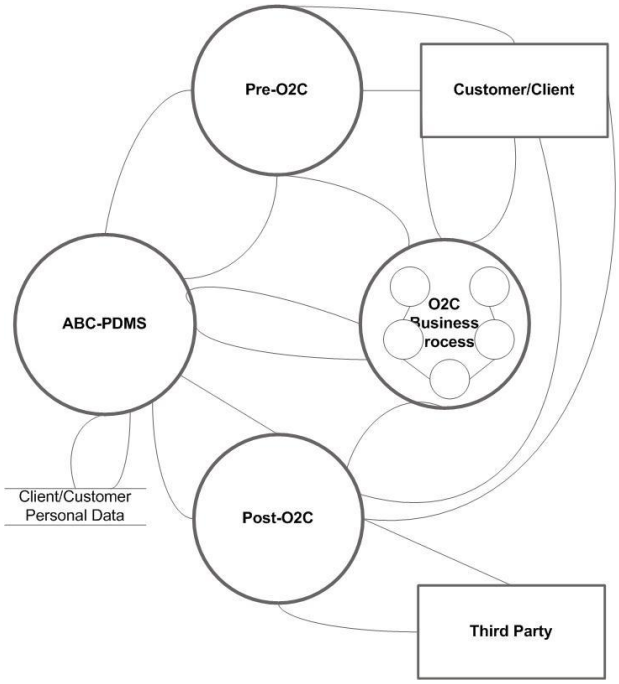

Figure 3. Integrating ABC-PDMS into O2C

The pre-O2C phase is very important since it presents a level of confidence by the client that the personal data collection process will be controlled per the organization's PPC. In this phase, a new client will be introduced to the **"receive"** and **"collect"** processes of the ABC-PDMS. This will guarantee that the personal data will be collected in compliance with the government legislation, policies and procedures of the organization, and the control mechanisms established in the organization. The client will acknowledge (via e-mail and m-commerce capabilities) the reading and approving of the PPC and provide his/her personal data accordingly. The collected data will be stored in the personal data file for future usage. A returning client will be introduced to an updated PPC in case the statement has been updated to receive his/her approval, otherwise the returning client will be handled to the O2C process. The O2C process will be activated and interact with the client as per the steps defined above. Any personal data processing during the O2C order fulfillment, shipping & delivery, invoicing & billing, and payment will be handled to the ABC-PDMS to ensure compliance with organization's own policies and procedures.

In the post-O2C phase, a client will have control on the usage of his/her data by integrating the **"accurate"**, **"access"**, and **"disseminate"** processes into the data management system. So, a client will be able to log into his/her account to make any changes,

will be engaged in any dissemination of his/her information, and be informed and getting his/her acknowledgement in case the organization plans to send his/her information to a third party.

7. Implications for Practice and Future Research

As per the results of the surveys mentioned earlier, it is clear that online customers are not happy about how governments and organizations are treating their personal data. Also, organizations are missing huge opportunity to gain the trust of such individuals to help in increasing their sales and customer satisfaction. The proposed solution will increase the trust of customers in the way organizations and governments are dealing with their data and will help in increasing the customer confidence and in turn increase the sales of online products and services and participation on online activities. As such, the proposed solution will have a crucial effect on practice. Further work should attempt to show how integration methods of privacy into the business processes used in this study is appropriate across all business processes. The proposed approach has not been implemented in real world applications. It presents a conceptual framework based on a design science approach. It does not include empirical validation of the framework. Future research should endeavor to validate the framework developed in this study. Another area for research is to develop business process controls for the ABC-PDMS. Such control will provide assurance about the quality of the data collection process and the accuracy process. Control systems enable management to meet this responsibility. For example, for the U.S. government agencies to be compliant with FISMA, Personal Identifiable Information (PII) controls should be developed in the ABC-ADMS to prevent the storage of data that can be used to uniquely identify an individual or can be used with other data sources to uniquely identify a single person.

This paper is one of very few to apply the sciences of design methodology with its three cycles to information systems research. As such, this paper will have huge impact on the body of knowledge not only for the study of privacy but also the field of design science research in information systems.

8. Conclusion

The importance of personal data protection is putting a heavy weight on both governments and organizations to come up with convincing solutions to customers that their data is protected and will be used only for the purpose it has been collected for in addition to provide the customers with full control of their own data. In line with this requirement, we have argued in this paper that data protection should be integrated in the business processes of the enterprise and control development should be integrated within systems development for process-centric personal data management system. The lack of an established approach and methodologies for the personal data protection has a huge effect on the number of customers involving in conducting business on the Internet. By using the sciences of design methodology, we have attempted a modest effort in this paper by proposing an integration of personal data into the business process of the enterprise. Though conceptual developments in this paper have been limited to requirements analysis and high level design, they could easily be extended to cover system design and implementation as well.

While embedding privacy modules has seen a development in terms of enterprise solutions offered by Enterprise system providers, a structured approach to privacy within enterprise environments is still lacking. This work has attempted to fill the gap by proposing the ABC-PDMS model. In summary, the ABC-PDMS consists of three domains, five processes, and the privacy services associated with them. All ABC-PDMS should be developed during the

analysis, design, and implementation phases of the system development life cycle. Therefore, This study has three objectives: ***(obj1)*** build an advanced business-centric personal data management system (ABC-PDMS) on the principle of predefined components; ***(obj2)*** facilitate the integration between personal data management system and business information processing within an enterprise using different building blocks; and ***(obj3)*** give organizations insight into how the proposed personal data management system help organizations to develop data protection in their business processes and to enhance their performance.

The approach used in this paper was simply modest and illustrative and not exhaustive in any ways. Several authors (CF. Kokolakis *et al*. 2000 and Carnaghan, 2006) propose different modeling and design techniques to support a more rigid integration between process-centric systems that can be used for the ABC-PDMS.

References

Anderson, J. and Rachamadugu, V., 2008. Managing security and privacy integration across enterprise business process and infrastructure. *IEEE International Conference on Services Computing,* 2, pp.351-358.

Aston University, 2001. Data protection policy and code of practice, June 2001. Available at: <http://www1.aston.ac.uk/EasySiteWeb/GatewayLink.aspx?alId=6607> [Accessed 30 June 2013].

Carnaghan, C., 2006. Business process modelling approaches in the context of process level audit risk assessment: An analysis and comparison. *International Journal of Accounting Information Systems*, 7, pp. 170-204.

Clarkson, K., Miller, R., Jentz, G., and Cross, F., 2009. *Business law text and cases, legal, ethical, global, and e-commerce environment*. Eleventh Edition. Mason, OH: South-Western, Cengage Learning.

Federal Trade Commission (Bureau of Consumer Protection) (FTC), 2010. A preliminary FTC staff report on protecting consumer privacy in an era of rapid change: A proposed framework for businesses and policymakers. Available at: <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf> [Accessed 1 May 2013].

Feigenbaum, J., 2010. Accountability as a driver of innovative privacy solutions. Available at: <http://www.law.yale.edu/documents/pdf/ISP/Feigenbaum_Accountability.pdf> [Accessed 20 March 2013].

FISMA, 2006. FY 2006 report to congress on implementation of the federal information security management act of 2002. Available at: <http://www.whitehouse.gov/omb/inforeg/reports/2006_fisma_report.pdf> [Accessed 1 May 2013].

Gartner, 2008. 2008 Data breaches and financial crimes scare consumers away. September 2008. Available at: <http://www.internetretailing.net/news/data-theft-concerns-beginning-to-hit-internet-shopping-volumes> [Accessed 2 October 2011]

Gelinas, U., Sutton, S., and Federowicz, J., 2004. *Business process and information technology*. Ohio: South-Western.

Hevner, A., 2007. A three cycle view of design science research. *Scandinavian Journal of Information Systems*, 19(2), pp. 87-92.

Hevner, A., March, S., Park, J., and Ram, S., 2004. Design science research in information systems. *MIS Quarterly*, 28(1), pp.75-105.

Kokolakis, S.A., Demopoulos, A.J., and Kiountouzis, E.A., 2000. The use of business process modelling in information systems security analysis and design. *Information Management & Computer Security*, Vol. 8(3), pp.107-166.

Laudon, K.C. and Traver, C.G., 2008. E-Commerce, business, technology, society. Fourth Edition. London: Pearson International.

Lwin, M.O., Wirtz, J., and Williams, J.D., 2007. Consumer online privacy concerns and responses: A power-responsibility equilibrium perspective. *Journal of the Academy of Marketing Science*, 35(4), pp. 572-585.

Majdalawieh, M., 2010. The integrated privacy model: Building a privacy model in the business processes of the enterprise. *The International Journal of Information Security and Privacy (IJISP)*. 4(3), pp.1-21.

Organization for Economic Cooperation and Development (OECD), 1980. Guidelines governing the protection of privacy and transborder flows of personal data. 23 September 1980.

Peffers, K., Tuunanen, T., Rothenberger, M., and Chatterjee, S., 2008. A design science research methodology for information systems research. *Journal of Management Information Systems,* 24(3), pp.45–77.

Peslak, A.R., 2005a. Privacy policies: A framework and survey of the fortune 50. *Information Resources Management Journal,* 18(1), pp.29-41.

Peslak, A.R., 2005b. Privacy policies of the largest privately held companies – A review and analysis of the Forbes private 50. Proceedings of ACM SIGMIS Conference 2005, Atlanta, Georgia, April 14-16, 2005.

Peslak, A.R., 2006. Current privacy issues and factors: Development and analysis. *Journal of Information Technology Impact*, 6(3), pp.171-186.

Peslak, A.R., 2007. *Progress in internet privacy policies: A review and survey of US companies from 1998 through 2006*. Chapter 12. In: M. Khosrow-Pour, ed. *Emerging information resources management and technologies*, Vol. 6. Hershey, PA: Idea Group Inc.

Pirim, T., James, T., Boswell, K., Reithel, B., and Barkhi, R., 2008. An empirical Investigation of an individual's perceived need for privacy and security. *International Journal of Information Security and Privacy*, 2(1), pp.42-53.

Serwin, A.B., 2010. The federal trade commission and privacy: Defining enforcement and encouraging the adoption of best practices - version 2.0. December 31, 2010. Available at: <http://ssrn.com/abstract=1733217> [Accessed 1 May 2013].

Teifke, L., 2003. The importance of privacy. Vice President, ALLTEL information services, 3/17/2003. Available at: <http://www.bankersonline.com/vendor_guru/alltel/alltel_privacy.html> [Accessed 1 May 2013].

The Office of Management and Budget (OMB), 2003. OMB guidance for implementing the privacy provisions of the e-government act of 2002. September 26, 2003. Available at: <http://www.whitehouse.gov/omb/memoranda_m03-22/> [Accessed 1 May 2013]

Thomas, R.E. and Maurer, V.G., 1997. Database marketing practice: Protecting consumer privacy. *Journal of Public Policy & Marketing*, 16, pp.147-55.

TNS and TRUSTe, 2008. Internet users' knowledge, attitudes and concerns about behavioral targeting and its implications on their online privacy. March 26, 2008. Available at: <http://www.truste.org/about/press_release/03_26_08.php> [Accessed 1 May 2013]

W3C, 2007. The Platform for Privacy Preferences Project (P3P). Available at: <http://www.w3.org/P3P/> [Accessed 1 May 2013]

Web Design Directory, 2005. Consumers fret about online ID theft but still don't protect themselves. 2005-08-05. Available at: <http://www.designdir.net/newsst_1440.html> [Accessed 1 May 2013].

Westin, A.F., 1967. *Privacy and freedom*. New York: Atheneum.

Williams, A.-L., 2003. Privacy matters – Why you need to pay attention now. September 25, 2003. Available at: <http://www.dww.com/?page_id=1060> [Accessed 1 May 2013].

Wipro BPO Ltd., 2008. Improving order-to-cash cycle. White Paper, Nov 2008. Available at: <http://www.wipro.com/Documents/resource-center/library/order2cash_in_telecom_mmi_a_nov0807.pdf> [Accessed 1 May 2013].