Controlling and Disclosing your Personal Information

NORJIHAN ABDUL GHANI[1], ZAILANI MOHAMED SIDEK[2]
[1]Information Science Department
University of Malaya
50603 Kuala Lumpur
MALAYSIA
norjihan@um.edu.my

[2]Centre for Advanced Software Engineering (CASE),
Universiti Teknologi Malaysia,
City Campus, Jalan Semarak,
54100 Kuala Lumpur,
MALAYSIA
zailani@citycampus.utm.my

Abstract: - As organizations come to rely on the collection and use of personal information in order to complete the transactions and providing good services to their users, more and more user personal information is being shared with web service providers leading to the need to protect the privacy. Personal information is processed, stored and disclosed and often it generated in the course of making a commercial exchange. Credit card numbers, individual identity number, purchase records, monthly income, and related types of personal information all have important role with his this commercial information system. However this creation and use of personal information raises issues of privacy not only for the individual, but also for organizations. Easy access to private personal information will cause the misuse of data, no control over the information and others. Because of this, it's important to protect the information not only from external threats but also from insider threats. Data disclosure when performing a task in web-based application should be ensured. Within the electronic scenario, personal information have been collected, stored, manipulated and disclosed without the owner's consent. This paper will discuss on the relationship between personal information and its privacy. We also extended the model introduced by Al-Fedaghi as a way to control the personal information disclosure. We also suggested that the use of Hippocratic Database concepts as a way to control the personal information disclosure.

Key-Words: - personal information, privacy, personal information flow model, Hippocratic Database

1 Introduction

During the past decade, there has been an increasing number of personal information that is being collected, used and disclosed, and the expansion of the World Wide Web has significantly facilitated to this growth. Today, more people rely on electronic commerce in their daily tasks. People not only buy groceries, booking air tickets via online applications but many other tasks can be done by using e-commerce applications. Today, the emerging trends of e-commerce have made more convenient and easy for people to do anything online. Data privacy is growing concern among businesses and other organizations in a variety sectors. Every day, these organizations are entrusted with the responsibility of managing personal information..

In [10], said that personal information has become the "basic fuel" for modern businesses and governments to carry out their services (as cited in [1]). Personal informationi is processed, stored and disclosed and often it generated in the course of making a commercial exchange. Credit card numbers, individual identity number, purchase records, monthly income, and related types of personal information all have important role with his this commercial information system. Such parties is collecting, analyzing, storing and sharing more personal information. Information about individuals is currently maintained in thousands of databases, with much of that information is replicated across multiple databases. It is estimated that information

on a particular person is stored in approximately 1000 different databases [18].

However this creation and use of personal information raises issues of privacy not only for the individual, but also for organizations. Easy access to private personal information will cause the misuse of data, no control over the information and others. Unfortunately, people do not realize that once they gave their personal information, they no longer have authorities to control it. People have lost their ownership once they released their personal information. They do not have their privacy towards their personal information anymore. The more personal information has been disclosed, the less privacy they have. It causes the ability to protect information and privacy policies enforcement becomes more important. The main issue here is, people have less control over what types of information about them have been collected, used, stored and disclosed by various agencies, both by private and government sectors. Because of this, it's important to protect the information not only from external threats but also from insider threats. Data disclosure when performing a task in web-based application should be ensured by data security mechanisms. Supposedly, each individual should own, maintain and control his own personal information, allowing access to those who needed his/her information for a certain purposes needed at that time of needed.

Unlike data security, which focuses primarily on preventing unauthorized individuals from inappropriately obtaining information, the privacy problem focuses on providing individuals the ability to control how their data is managed and used by a particular organization. Violations of personal information privacy also called data protection occurred when personal information is improperly collected, used or disclosed. In [19], Westin stated that there are three statements on how people agree or disagreed about personal information privacy concerns:

1. Consumers have lost all control over how personal information is collected and used by companies
2. Most businesses handle the personal information they collect about consumers in a proper and confidential way
3. Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.

Because of this reason, personal information privacy preserving is a growing challenge for database security and privacy experts. Privacy preserving is a process of finding appropriate balances between privacy and multiple competing interests [6].

The rest of this paper is as follows; Section 2 will give an overview of personal information and its relationship with privacy. It also covers the importance of privacy for personal information. Section 3 explains the OECD's principles that have been adopted as guidelines in this paper, and Section 4 continues the discussion on the extended personal information flow model introduced in [2].

2 Personal information and Privacy

This section will briefly discuss on personal information and its privacy. Before we explained further on personal information, we should understand the meaning of privacy.

2.1 Privacy

The way people do business has been changed by the advancement in information technology, from off line transaction to online transaction. Most people are relying on online shoppersonal informationing, e-government, online banking for their daily tasks. By changing the way of transaction, people can obtain more advantages. Because of that, we are in the era of information overload. Forced by consumer demands and market competition businesses feel the need to collect more information from the people. This may help them to achieve the efficiency to the organizations. But, on the other hand, the concern of privacy is a main reason for people not willing to trade online who are otherwise willing to do if their privacy is assured.

It's important to ensure the data security and privacy in information system, specifically in today's web-based applications. Let us differentiate between privacy, confidentiality and security. [20] differentiate between privacy, confidentiality and security :

> **Privacy** is a social, cultural and legal concept, all three aspects of which vary from country to country.
>
> **Confidentiality** is a managerial responsibility: it concerns the problems of how to manage data by rules that are satisfactory to both the managers of data banks and the persons about whom the data pertain.
>
> **Security** is a technical issue. It focuses on how the rules of data access established by management can be enforced, through the use of passwords, cryptography, and like techniques.

Internet users want and expect privacy when conduct the transaction electronically. The notion of privacy is becoming an important feature in all aspects of life in modern society especially when it comes to confidential information disclosure. As explained in the previous section, privacy is a concern about the disclosure of confidential information, normally refers to personal informationi. Privacy protection is needed to avoid the inappropriate utilization and unlawful uses of personal informationi. Privacy will be to the information economy of the next century what consumer protection and environmental concerns have been to the industrial society of the 20th century [21]. New technologies worldwide have affected different aspects of dealing with private information in the areas of security, commerce, government, etc.

There have been many efforts to define privacy. This difficulty in defining a single definition of privacy has resulted in multidimensional approaches in defining it. It can be defined in various contexts such as legal and economic. In a legal context, privacy is largely synonymous with a right to be let alone [22]. From the economic context, privacy is defined as the concealment of useful information assuming an economic value in transaction (Stigler, 1980).

Different people have different views regarding privacy. Kang in [23] claimed that privacy involves the control of the flow of personal informationi in all stages of processing – acquisition, disclosure, and use. In [24], privacy is defined as an ability to control collection, retention and distribution of them. Burgoon, *et al.* In [25] defines privacy as "the ability to control and limit physical, interactional, psychological and informational access to the self or one's group. Privacy is defined as the right of individuals to determine for themselves when, how and to what extent information about them is communicated [19]. The panel on Privacy and Behavioral Research of the Office of Science and Technology defined privacy in this way :

> *The right to privacy is the right or the individual to decide for himself how much he will share with others his thoughts, his feelings, and the facts of his personal life. It is a right that is essential to insure dignity and freedom of self-determination.*[1]

Al-Fedaghi, in [26] discussed the difference between secrecy and confidentiality. He stated that "confidential" information generally refers to any information that must be kept in confidence such that its reveal requires the consent of its owner. It implies protection of other's people's secrets through the control of access to information and its release according to certain agreement. Here, from a various definition above and the statement by Al-Fedaghi (2005a), we can conclude that privacy is a base for confidentiality.

2.1.1 Categories of Privacy

Some authors categorized the privacy in two categories. [28] differentiate between information privacy and communication privacy. Johnson *et al*, in [27] differentiate information or database privacy issues from communications privacy by placing in the latter category the set of privacy concerns related to technologies such as electronic surveillance, encryption, email and digital telephony. Information security issues are those associated with personal informationi stored in a database. Several types of privacy have been distinguished in literature including physical privacy and informational privacy [6].

Al-Fedaghi, in [29] conceptualized privacy into two categories; 1) *personal informationi privacy* and 2) *non-personal informationi privacy*. The non-personal informationi privacy may be sub-categorized based categorizations of privacy that include such privacy types as physical privacy meanwhile personal informationi privacy involves acts on personal informationi. From this classification, we noticed that, there are two types of privacy; information privacy and non-information privacy. Non-information privacy can be a part of physical privacy or communications privacy.

In [6], Clarke claims that there are several dimensions of privacy:

- *privacy of the person*, sometimes referred to as 'bodily privacy'. This is concerned with the integrity of the individual's body. Issues include compulsory immunization, blood transfusion without consent, compulsory provision of samples of body fluids and body tissue, and compulsory sterilization;
- *privacy of personal behavior*. This relates to all aspects of behavior, but especially to sensitive matters, such as sexual preferences and habits, political activities and religious practices, both

[1] Executive Office of the President, Office of Science and technology, Privacy and Behavioral Research, Washington, D. C., 1967

in private and in public places. It includes what is sometimes referred to as 'media privacy';

- *privacy of personal communications*. Individuals claim an interest in being able to communicate among them, using various media, without routine monitoring of their communications by other persons or organizations. This includes what is sometimes referred to as 'interception privacy'; and
- *privacy of personal data*. Individuals claim that data about themselves should not be automatically available to other individuals and organizations, and that, even where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use. This is sometimes referred to as 'data privacy' and 'information privacy'.

2.2 Personal information

Data is important in any transaction; either off-line transaction or online transaction. Unfortunately, not many people realized and understand how important and valuable their personal information are. Some personal information can be classified as sensitive and need to be kept as private information. Some personal information are sensitive but there is no need to keep it private. There are four types of data involved in processing [3]:

i) *Personal data* : any data that can be used to identify a person such as name, address, telephone number.
ii) *Sensitive data* : any data that disclose information about racial or ethnic origin, religious, philosophical or other belief, political opersonal informationinion, membership of parties, as well as personal data disclosing health such as health history, race.
iii) *Identification data* : personal data that permit the direct identification of the data subject such as DNA, identity card number.
iv) *Anonymous data* : any data that cannot be associated to any identified or identifiable data subject such as gender, type of disease.

From the above classification, the first three types of data can be considered as private information. Private information is personal information that requires protection due to risks that could result from its disclosure, alteration, or destruction. This personal and private information should be protected to ensure the privacy.

Personal data will go through a process to become information. There are various definitions for personal informationi. In 1993, personal informationi is defined as any information that is related to the individual person. The personal information is often understood as individual information that is owned by a person, such as calendar notes, contact addresses of the friends and so on. Bergman et al. [30] defined it through personal information management (Personal information Management); it is the storage, organization, and retrieval by an individual for her/his own use. Heikkinen et al. [5] define personal informationi as any information that is related to the individual person. Personal informationi is any linguistic expression that has referent(s) of type person [4]. There are three categories of referent(s) :

- Zero personal information – having no individual referent
- Atomic personal information – having a single referent
- Compound personal information – having more than one referents

In web-based environment, personal informationi is disclosed by the data owner and used by the organizations. The organization will collect, store, manipulate information to fulfill their organizations' needs. From information system views, information privacy can protect individuals from misuse of data, or unauthorized access to, or modification of information could adversely affect, or be of risk to the owner of that information. Information play a fundamental role in privacy domain as they shall be collected, manipulated, stored, and disclosed according to their needs. Clarke, in [6] define privacy as follows:

> "*the interest that individuals have in sustaining a 'personal space', free from interference by other people and organizations.*"

2.3 Types of Personal information

In [8], there are two types of personal informationi; *1)* private personal informationi and *2)* non-private personal informationi. Private personal informationi refers to uniquely identifiable individual of a possession of a person meanwhile non-private personal informationi is doesn't refer to uniquely identifiable person. Private information is any information that includes his/her own private information. Non-private information is any information that is owned by a person but not considered as private

information, such as calendars, maps, business notes, and others. For our research purposes, we may refer to the first type of personal informationi; private personal informationi. To avoid any confusing, we will refer it as private personal informationi.

Personal information should be kept by the owner itself or control the disclosure in order to ensure its privacy. But, in web-based application, this information should be disclosed in order to fulfill the transaction. Although the private information is being disclosed, normally, for the security and privacy reason, it should not be accessed by unauthorized users. For this reason, there are three main issues that need to be considered:

i) personal informationi should not be accessed by unauthorized users,
ii) only required personal informationi will be posed,
iii) personal informationi cannot be passed to those who do not need the information.

2.4 Personal Information Privacy

Personal information privacy is an "individual's claim to control the terms under which personal informationi – information identifiable to the individual – is acquired, disclosed and used."[2] This definition comes from Principles for Providing and Using Personal informationi ("IITF Principles") issued by the Clinton administration's Information Infrastructure Task Force.

Jajodia, (1996) introduced five basic principles in order to achieve information privacy :

i) *Proper acquisition and retention* is concerned with what information about individuals is collected and how long the information is kept by an organization.

ii) *Integrity* is concerned with maintaining information about individuals that is correct, complete, and timely.

iii) *Aggregation and derivation of data* is concerned with ensuring that any aggregation or derivations performed by an organization on its information are necessary to carry out its responsibilities.

iv) *Information sharing* is concerned with authorized or proper disclosure of information to outside organizations or individuals. Information should be disclosed only when specifically authorized and solely for the limited use specified.

v) *Proper access* is concerned with limiting access to information and resources to authorized individuals who have a demonstrable need to perform official duties. Thus, information should not be disclosed to those who are either not authorized or do not have a need to know (even if they are authorized).

To understand how to achieve information privacy, we must understand how it's violated. Information privacy is violated when personal informationi is collected unbeknownst to individuals and when personal informationi, which may have been given freely and knowingly, is later used or disclosed in a manner outside the original agreement or understanding. Awareness of the collection of personal informationi is a first step I achieving information privacy. In other words, controlling the flow of one's personal informationi starts at the point of collection. Once an individual chooses to release some portion of his or her personal informationi, the individual must rely on laws or mechanisms to control the further distribution and subsequent use of that information.

2.5 Privacy-preserving Information Management

Data represent an important asset to an organization, especially for today's businesses where most organizations are moving towards online applications. Because of that, we see an increasing number of organizations that collect data, normally personal information and use them for various purposes. Sometimes, organizations may give access to the data or reveal it another third party. This wills posses serious privacy threats against the privacy protection for individuals and organizations. Because privacy is an important concerns, several research effort have been carried out; referred as privacy-preserving data management techniques. There are three privacy-preserving data management techniques have been addressed; data anonymization, data mining and database tailored to privacy policy. The next subsection will discuss further these three techniques.

2.5.1 Data Anonymization

A first technique deals with privacy-

[2] IITF Principles,

preservation when data are to be released to third parties. Data once released are no longer under the control of the individual or organizations owning them. Therefore, the organizations are unable to control the way data are used after released it. The most common approach is to modify the data by removing all information that can directly link data items with individuals; referred to data anonymization.

2.5.2 Privacy Preserving Data Mining

A technique deals specifically with privacy-preservation in the context of data mining. The use of data mining techniques may allow one to recover the removed information. Several approaches have been proposed such as tools for association rule mining or classification systems. In general, all approaches are based on modifying or perturbing the data in some way; for example, techniques specialized for privacy-preserving mining of association rules modify the data so to reduce the confidence of sensitive association rules.

2.5.3 Database tailored to Privacy Policy

Finally, some preliminary efforts have been reported dealing with database systems specifically tailored to support privacy policies, such as the policies that can be expressed by using the well-known P3P standard. In particular, Agrawal, *et al.* [31] have recently introduced the concept of Hippocratic Database, incorporating privacy protection in relational database systems. They introduce the fundamental principles underlying Hippocratic Database and propose the Strawman Architecture. An important feature of this architecture is defining privacy metadata consist of privacy policies and privacy authorizations. The Hippocratic database performs privacy checking during query processing. In their paper, Agrawal, *et al.* [31] also discusses various technical challenges and problems in designing Hippocratic databases, such as efficiency, disclosure, retention, and safety.

3 OECD Principles

Over a few years ago, there are a number of guidelines exists to protect the PERSONAL INFORMATIONI. These guidelines are important to ensure the PERSONAL INFORMATIONI privacy. In 1980, the Organization of Economic Cooperation and Development or OECD, adopted and expanded eight principles as part of the "Guidelines on the protection of Privacy and Transborder Flows of Personal Data". The OECD has therefore been focusing on how these Guidelines may best be implemented in the 21st century to help ensure the respect of privacy and protection of personal data online. There are eight principles described by OECD's guidelines as follows [7]:

1) *Collection Limitation Principle*
   There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2) *Data Quality Principle*
   Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3) *Purpose Specification Principle*
   The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4) *Use Limitation Principle*
   Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except: *a)* with the consent of the data subject; or *b)* by the authority of law.

5) *Security Safeguards Principle*
   Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6) *Openness Principle*
   There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7) *Individual Participation Principle*
An individual should have the right:
   a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
   b) to have communicated to him, data relating to him
      - within a reasonable time;
      - at a charge, if any, that is not excessive;
      - in a reasonable manner; and
      - in a form that is readily intelligible to him;
   c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
   d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8) *Accountability Principle*
A data controller should be accountable for complying with measures which give effect to the principles stated above.

Next section will explain on how this guideline has been incorporated to personal information flow model. This guideline has been used as a guide to extend the work done by Al-Fedaghi, 2005.

4 Personal information Flow Model

Previous section discussed on OECD's principles that have been adopted to protect the personal information privacy. In [4], Hippocratic Database (HDB) is a database concept that adopted these eight principles to come out with ten principles to protect the personal information privacy in a database system. Personal information flow model (PIFM) has been introduced by Al-Fedaghi in [2, 8, 9] which consists of four main modules or phases; creating, collecting, processing and disclosing the personal information. This PIFM provides a systematic method of understanding related notions and explains a broad variety of cases by illustrating the relationship between different actors on personal informationi. The PIFM consists of four main phases which include informational privacy entities and processes, as shown in Figure 1. These four phases are creating personal informationi, collecting personal informationi, processing personal informationi and disclosing personal informationi.

Besides this four phases, we decided that it is important to control the personal information before disclose it. Figure 1 shows an extended version of PIFM introduced by Al-Fedaghi. Al-Fedaghi, in his paper introduced four phases in PIFM. This model reflects the personal information pattern that guides and restricts relationship among objects (e.g., proprietors, possessors, miners) and phases [2]. The purpose is to show the relationship of recognizing, understanding and manipulating personal information. This model complements other descriptions such as the data protection EU directive as an explicit representation of personal information flow in realty. EU directive lumps together all processing of personal data to mean collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction [2].

Dorsey, in [32] introduced different types of categories applied to information mentioned in personal information: retrieving information, evaluating/assessing information, organizing information, analyzing information, presenting information, securing information, and collaborating around information (as cited in Al-Fedaghi, [2]. In the context of personal information privacy, this category can be applied to several phases such as creating, collecting, processing, controlling and disclosing the personal information.

But, in a way to protect the personal information, there is a need to control the personal information disclosure. Because of that, we add one phase between processing and disclosing personal information. An extended model was carried out to adopt the principles introduced by OECD "Guidelines on the protection of Privacy and Transborder Flows of Personal Data" discussed above. This model stated that any personal information should be disclosed only to authorize users, with a specific purpose and for a limited time. Because of this reason, we add another phase named "*Controlling the personal information*" before "*Disclosing the personal information*" phase.

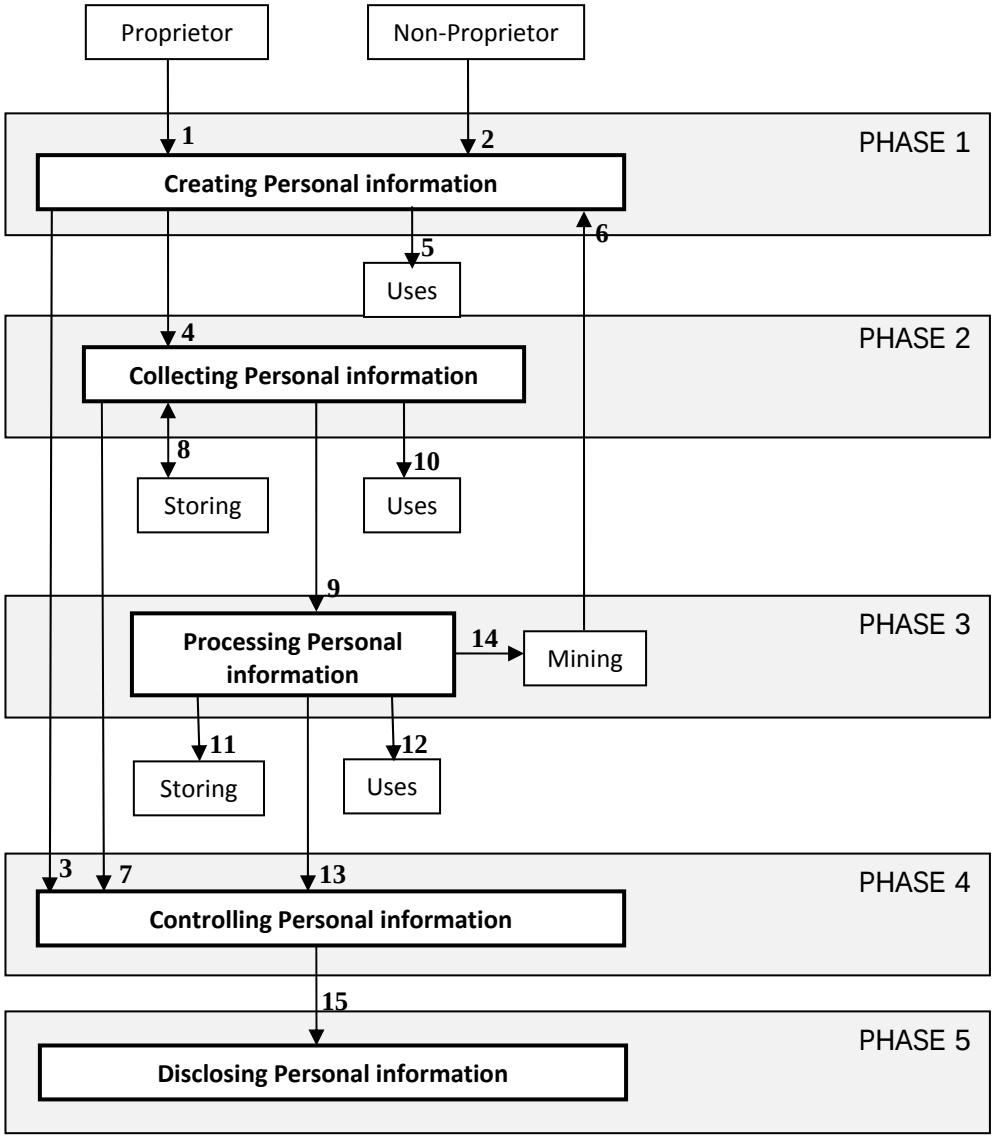

Figure 1: Enhancement of PIFM introduced by Al-Fedaghi, (2006b,2006c)

As in Figure 1, there are five main phases in PIFM. These five phases explain how the personal information is created, collected, processed, controlled and disclosed.

4.1 Creating personal information

Creating personal information is the first phase on the PIFM. Personal information can be created by two parties; proprietor and non-proprietor (e.g. medical diagnostic procedures performed by physicians) or by deduced by someone (e.g. data mining that generates new information from existing information) [2]. Figure 1 shows that personal information can be created at point labeled 1, 2 and 6. Any atomic personal information of an individual is proprietary personal information of its proprietor. Once the personal information have been created, it can be either used (point 5) or collected (point 4) or go to controlling phase before disclose it (point 3). Uses means that the personal information is used in decision making process. Point 3 stated that the personal information should be controlled before disclosed. It means that the personal information will only be disclosed if it passes the fourth phase.

4.2 Collecting Personal information

After the personal information is created, it can be collected at point 4. Personal information is collected from various sources and for various purposes of

collection. The collected personal information can be either kept as records for future used (point 8), used it (point 10), process the personal information (point 9) or proceed to controlling phase (point 7).

4.3 Processing Personal information

The processing phase of personal information involves acting like storing (point 11), using (point 12) and mining (point 12) the personal information. Personal information is processed based on the purpose it being collected. Besides this the personal information can also be controlled (point 13).

4.4 Controlling Personal information

Previous model introduced by Al-Fedaghi is modeled without "controlling personal information phase". In this paper, we extended the work done by him by adding this phase. In this new era of internet, it is important to control the personal information before disclosing it. This phase will check the personal information before it goes to the last phase; disclosing the personal information. Figure 1 shows all the personal information are controlled at point 3, 7 and 13 before deciding either the personal information can be disclosed or not.

4.5 Disclosing Personal information

Disclosing personal information meaning that the personal information is going to be released to insiders or outsiders. Personal information is only being disclosed if it is authorized to do so.

5 Conclusions

In this paper, we extended the work done by Al-Fedaghi on personal information flow model. This model was designed to control the personal information disclosure. Personal information should be disclosed only to authorize users with specific purposes for a limited time.

References:

[1] Al-Fedaghi, S. Personal information eWallet, *2006 IEEE International Conference on Systems, Man, and Cybernetics*, October 8-11, Taipei, Taiwan. (2006a).

[2] Al-Fedaghi, S. Aspects of Personal information Theory, *Proceedings of the 2006 IEEE Workshop on Information Assurance*, United States Military Academy, West Point, NY. (2006b).

[3] P. Guarda, N. Zannone, Towards the development of privacy-aware systems. Inform. Softw. Technol. (2008).

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

[5] Heikinen, K., Juha E., Pekka J., and Jari, P. Personalized View of personal informationi. *WSEAS Transactions on Information Science and Applications*, vol. 2, No. 4, 2004.

[6] Clarke, R. 1999. Introduction to Dataveillance and Information Privacy, and Definitions and Terms.[Online] Available : http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html#Priv.

[7] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OECD Publications, Paris. Available online at : http://www.uhoh.org/oecd-privacy-personal-data.PDF.

[8] Al-Fedaghi, S. Personal Management of Private Information. Innovations in Information Technology, 2006. Pp 1-5. (2006).

[9] Sabah Al-Fedaghi, "Personal informationi Flow Model for P3P", W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement, Ispra Italy, October 17-18, 2006.

[10] Perri, 6, The Future of privacy. Volume 1:Private Life and Public Policy, Demos, London, 1998

[11] Dorsey, P/ (2000). What is PKM? http://www.millikin.edu/webmaster/seminar/pkm.html.

[12] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu. Hippocratic databases. In *The 28th International Conference on Very Large Databases (VLDB)*, 2002.

[13] EU Directive 95/46/EC – The Data Protection Directive, http://www.dataprotection.ie/viewdoc.asp?m=&fn=/documents/legal/6aii-2.htm#5.

[14] Skinner, G., Han, S. & Chang, E. (2006). A conceptual framework for Information Security and Privacy. *Proceedings of the 5th WSEAS International Conference on Applied Computer Science*, Hangzhou, China. April 16-18, 2006. pp410-415.

[15] Skinner, G., Han, S. & Chang, E. (2006). A conceptual framework for Information Security and Privacy. *Proceedings of the 5th WSEAS International Conference on Applied Computer Science*, Hangzhou, China, April 16-18, 2006. pp981-986.

[16] Papathanassiou, A. E., Mamakou, X. E. & Kardaras, D. K. (2006). Privacy Online: Research and Recommendations. *Proceedings of the 5th WSEAS International Conference on Telecommunications and Informatics*, Istanbul, Turkey, May 27-29, 2006 (pp309-314).

[17] Ali, H. (2005). Security & Trust in Agent-enabled E-commerce : Survey. *Proceedings of the 4th WSEAS Int. Conf. on Information Security, Communications and Computers*, Tenerife, Spain, December 16-18, 2005 (pp1-6).

[18] Brands, S. A. (2000). *Rethinking Public Key Infrastructures and Digital Certificates : Building in Privacy*. Cambridge, Massachusetts,o. Document Number).

[19] Westin, A. (1967). *Privacy and Freedom*. Atheneum, New York.

[20] Gotlieb, C. C. (1995). Privay : A Concept Whose Time Has Come and Gone. In D. Lyon & E. Zureik (Eds.), *Surveillance, Computers and Privacy* (pp. 156-171): University of Minnesota Press.

[21] Gleick, J. (1996, September 29, 1996). Behind Closed Doors; Big Brother is Us. *New York Times*.

[22] Warren, S., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review. *Vol. IV December 15, 1890 No. 5* Retrieved July 19, 2008, from http://www.lawrence.edu/fast/boardmaw/Privacy_brand_warr2.html.

[23] Kang, J. (1998). Information Privacy in Cyberspace Transactions. *Stanford Law Review, 50*, 1193.

[24] Goldberg, I., Wagner, O., & Brewer, E. (1997). *Privacy-Enhancing Technologies for the Internet.* Paper presented at the IEEE COMPCON '97.

[25] Burgoon. (1989). Maintaining and restoring privacy through communication in different types of relationship. *Journal of Social and Personal Relationships, 6*, 131-158.

[26] Al-Fedaghi, S. S. (2005a). *Privacy as a Base for Confidentiality*. Paper presented at the Fourth Workshop on the Economicx of Information Security.

[27] Johnson, D. G., & Nissenbaum, H. (1995). *Computers, Ethics & Social Values* (1995 ed.). Englewood Cliffs, NJ: Prentice Hall.

[28] Tavani, H. T. (1999). Privacy Online. *Computers and Society*, 11-19.

[29] Al-Fedaghi, S. S. (2007a). Anatomy of personal information processing: application to the EU privacy directive. *International Journal of Liability and Scientific Enquiry, 1*(1), 129 - 138.

[30] Bergman, O., Boardman, R., Gwizdka, J., & Jones, W. (2004). *Personal Information Management* Paper presented at the ACM Conference on Human Factors in Computing Systems.

[31] Agrawal, R., Kiernan, J., & Srikant, R. (2002a). *Hippocratic Database.* Paper presented at the 28th International Conference on Very Large Data Bases, Hong Kong, China.

[32] Dorsey, P. (2000). What is PKM? Retrieved 20 July, 2008, from http://www.milikin.edu/webmaster/seminar/pkm.html