Designing for Privacy from Islamic Perspectives Using Value Sensitive Design

Fadzlin Ahmadon[1], Rosmawati Nordin[2], and Rashidah Md Rawi.[3]

[1]*Universiti Teknologi MARA, Malaysia, fadzlinahmadon@gmail.com*
[2]*Universiti Teknologi MARA, Malaysia, roswati@tmsk.uitm.edu.my*
[3] *Universiti Teknologi MARA, Malaysia, rrawi@tmsk.uitm.edu.my*

ABSTRACT

One of the advantages of computerized record-keeping system is its ability to shield sensitive information from prying eyes. There are many system development methodologies to safeguard privacy and Value Sensitive Design is one approach that focuses on embedding moral values into technology design. Islamic traditions while supporting commonly regarded moral values such as justice and truth often has additional requirements for believers to fully uphold those values from Islamic perspective. Privacy is one such value. While in agreement on many techniques introduced by western scholars to safeguard privacy in system design, the unique concept of *awrah* as part of privacy consideration in Islam is one such additional reflection for system designers.

Keywords: value sensitive design, Islamic values, privacy.

I INTRODUCTION

Islam as a religion reaffirms the need to uphold moral values. It upholds human values as long as it is not in contradiction with Islamic teachings. In regards to this, Islamic teachings can be used as a framework to base ethical considerations not unlike using Utilitarianism or Virtue approaches to make decisions (Velasquez et al., 1996). Differing from mainstream ethical frameworks that can result in different or even opposing decisions as is always the case with Utilitarianism versus Virtue approach (Fleurbaey & Maniquet, 1997), decision based on Islamic values however are more constant. This is because the modern world has a relative concept of good and evil while Islamic ethical values are grounded from the two sources of Qur'an and Sunnah (Mamat, 2008).

While Islam promotes the same good values that mainstream ethical views do, there are differences in its execution. In the case of privacy, Islam respects the need of privacy, and extends the concept to include respect to modesty and cross-gender interactions as per the concept of *awrah (*Padela & del Pozo, 2011).

In order to address privacy concerns from Islamic perspectives especially when resulted system involves Muslim users either in direct or indirect ways, considerations must be done even from the designing stage. This is because technology is not morally neutral (Brey, 2000) or simply a tool where ethical or unethical behaviors can be performed on. Designers are responsible in creating the conditions that define the range and type of possible moral interactions. In simpler words, this means that designers shape the moral behavior of users within the system (Chapman, 2006).

One design approach that tackles the need for values consideration from the designing stage is Value Sensitive Design.

II PRIVACY IN DESIGN AND ISLAMIC PERSPECTIVE

Privacy, defined by the Merriam Webster dictionary as *"the quality or state of being apart from company or observation and freedom from unauthorized intrusion*" ("privacy," 2012) is a design goal for many information systems. In fact, one of the earliest literature written on the issues of information system usage written by Mason in 1986 highlighted the issue of privacy among others (Mason, 1986). Association of Computing Machinery, one of the world's largest associations of computing professionals also has "respect the privacy of others" in their Code of Conducts ("ACM code of ethics and professional conduct," 1992).

Privacy however is mostly seen as a non-functional requirement (NFR) for system development. As a contrast, functional requirements are the reasons why the system is needed at the first place such as "tasks the system should perform" (Yu & Cysneiros, 2002). However, according to Yu, Cysneiros (2002) failure to address NFR is one of the most expensive to correct.

In Islam, privacy as a fundamental right is respected and highly regarded. Among the most important messages on privacy is the need for asking for permission:

O ye who believe! Enter not houses other than your own, until ye have asked permission and saluted those in them: that is best for you in order that ye may heed (what is seemly). If ye find no one in the house enter not until permission is given to you: if ye are asked to go back, go back: that makes for greater purity for yourselves: and Allah knows well all that ye do. It is no fault on your part to enter houses not used for living in, which serve some (other) use for you: and Allah has knowledge of what ye reveal and what ye conceal. (Qur'an 24: 27-29)

The verse above also asserted that if permission was not given, one should go back and not attempt to go in.

Islam not only includes asking for permission and making oneself known, it also includes the prohibition of suspecting others of wrongdoings, spying on others and also spreading others' private information:

O ye who believe! avoid suspicion as much (as possible): for suspicion in some cases is a sin: and spy not on each other, nor speak ill of each other behind their backs. Would any of you like to eat the flesh of his dead brother? Nay, ye would abhor it...but fear Allah: for Allah is Oft-Returning, Most Merciful. (Qur'an 49:12)

Spying on others or espionage as prohibited in Islam is also extended by Al-Ghazali as "search for signs in order to know what is otherwise not known and not permitted by the *Shariah* (Kamali, 2008).

Respecting privacy in Islam also includes protecting the modesty of oneself as in the concept of *awrah*.

Awrah is areas of body that must be clothed and its regulation differs based on the audience one is in (Padela & del Pozo, 2011). The importance of protecting's one *awrah* is stressed in the Qur'anic verse:

O prophet! tell thy wives and daughters, and the believing women, that they should cast their outer garments over their persons (when abroad): that is most convenient, that they should be known (as such) and not molested: and Allah is Oft-Forgiving, Most Merciful. (Qur'an 33:59)

In addition to protecting the modesty of one, Islam also highlights respect to the privacy of others:

Say to the believing men that they should lower their gaze and guard their modesty: that will make for greater purity for them: And Allah is well acquainted with all that they do. (Qur'an 24:30)

Hence privacy in Islam does not only come as an edict but also with clear instructions and limits to be followed by believers.

III VALUE SENSITIVE DESIGN

Value Sensitive Design is a design approach that argues moral values should be embedded within a system design (Friedman, Peter H. Kahn, & Borning, 2002). This design method is made up of three iterative steps; conceptual investigation, empirical investigation and technical investigation.

In conceptual investigation, identification of direct and indirect stakeholders and how they are affected by the usage of technology is identified. In this step contemplation of values that are affected, value trade-offs and the development of working definitions on values of interest, drawing from works in ethics and philosophy are also done (Borning, Friedman, & Kahn, 2004).

In empirical investigation, the human context of the system is investigated. Any human activity that can be observed, measured or documented are investigated in this stage (Friedman, et al., 2002).

Technical investigation is divided into two steps, first recognizing on how current technology support or impedes moral values and the second step is the design works to support values identified in conceptual investigation (Friedman, et al., 2002).

IV CURRENT CONDITION

Study was done in the psychology clinic of a university hospital in an eastern coast state in Malaysia. Psychology progress record is highly confidential information and should only be made viewable to very few selected people. In the current situation however, every patient has their own file that consists of records and notes for every wards and clinics that he or she has been treated on. For example, if the patient was treated for cancer in the Oncology Department and was also referred to the Psychiatry Department later on, all of his medical records and notes are made available in the same file.

While Psychological Progress Records are filed with the header of "highly confidential", nothing is stopping prying eyes to try and read them. Having only one file per patient while being good in making sure all the information is in one place, brings the problem of the file being in other ward or department when it is being needed by the psychologist. It makes it hard for the psychologist to be prepared before receiving patients by reading records from previous sessions and sometimes the patient's file is not even at the Psychology Clinic when session is starting.

V DESIGNING USING VALUE SENSITIVE DESIGN

In addition to hindering the psychologist's work, current file-based system seriously compromise the privacy of psychology clinic's patients when psychologists are urged to take steps to establish and maintain confidentiality of information from their sessions (Association, 1993). In regards to this, a migration to computer-based record system can address some of the most pressing issues regarding compromising of patients' privacy and in this study the design of the computer system was done using the methods of Value Sensitive Design.

A. Conceptual Investigation

The most important part of this step is identifying the direct and indirect stakeholders of the eventual system. Direct stakeholders are the people who interact directly with the computer system while indirect stakeholders are referring to all parties who are effected by the usage of said system (Friedman, et al., 2002). Often indirect stakeholders are ignored during design process when in certain systems they are the ones who are mostly affected. This is especially true in the case of HUSM Psychology Clinic.

After interview sessions were conducted, the direct stakeholders of the system are recognized as such:

Psychologist is the main user of the system. Currently the psychology clinic has only one psychologist in charge, and the psychologist conducts her clinic on every Monday and Tuesday. The psychologist is attached to two departments, Psychiatry and Pediatric and is responsible for decision to accept patient for treatment, assigning of appointments, treatment plans, writing progress records and also writing reports on their psychological condition, where this reports may be required by the patients for official businesses such as registering for special needs class in school.

Psychiatrists are medical doctors who work in the Psychiatry Clinic in the university hospital. They are the ones who treat patients with psychiatric disorders, diagnose and also prescribe medications to the patients. In cases that the psychiatrists deem can benefit from sessions with psychologist, they will be referred to the psychology clinic. Some of these cases' progress records may be made available to them in order to facilitate discussions for better treatment of the patients.

Referrers are medical doctors that refer patients they are currently treating in the hospital, external referrers from hospitals other than subject hospital and also the references can also be received from the corporate arm of the university hospital. These referrers refer patients that they think can benefit from psychology treatments to the psychology clinic.

Staff Nurses work at the psychology clinic and help the psychologist in handling references, receiving patients at the clinic, assisting patients in filling up forms, calling up patients to remind them of their appointments and also other related clerical works at the clinic. Staff Nurses also help the psychologist in administering tests during sessions.

Indirect stakeholders meanwhile are the **psychology clinic's patients** and also **close friends and relatives** to the patient.

Privacy is the value of import that has been recognized to be designed into the system. In 2003, Organization for Economic Co-operation and Development (OECD) listed a set of principles governing the handling of personal information and dubbed it as "Privacy Principles". The principles are **collection limitation**, **data quality**, **purpose specification**, **use limitation**, **security safeguards**, **openness**, **individual participation** and **accountability** (OECD, 2003).

The importance of making a focus on privacy from the initial phase of system development was also stressed by Patil and Kobsa (2009). In their paper they have summarized design techniques that have been proposed by many other literatures in order to promote privacy in system design. These techniques include **encryption**, **access control via preferences policies and roles**, **mechanism to reduce burden of preference specification such as grouping and templates**, **automatic or manual control of the degree of details of disclosed information**, **implementing feedback**, **distortion**, and **support for anonymity** among others. While choosing only one technique may not be able to satisfy the system's privacy requirements, it was suggested combining a few of listed approaches is done (Patil & Kobsa, 2009).

In order to design this system, privacy design techniques from mainstream works is used in support of the defined privacy from Islamic sources.

B. Empirical Investigation

Human activities that are conducted at the clinic begin with receiving referrals. As of the current practice, referrals are received in the shape of written forms submitted to the staff nurses stationed at the clinic. Sometimes referrers would submit their referrals by calling or e-mailing the staff nurses or even the psychologist and they would fill up the reference form on behalf of the referrers.

If a reference is accepted by the psychologist, the patient will attend clinic sessions at the psychology clinic. If it is the patient's first time for receiving

treatment in HUSM, a new file will be created for the patient. However, if the patient previously received or is currently receiving treatment at the hospital, the staff nurse must retrieve the patient's file from other ward first.

During treatment session, psychologist will fill in the patient's progress note. Once the session is done, the document will have to be filed under the segment of the clinic or ward the patient was referred from in the patient's file.

C. Technical Investigation

The initial conceptual investigation delineates the need for a better system to be used in the Psychology Clinic. Current concept of paper-based file though convenient for doctors doing their rounds at hospital wards bring up the issues of infraction of patients' privacy especially regarding the highly sensitive information contained in their psychological progress note.

Design works were done to satisfy the privacy requirements that safeguard patient's privacy. Using the design principles from mainstream literatures and Islamic sources, an online system for Psychology Clinic Information System were developed.

VI RESULTS

The system developed employs several design features to safeguard privacy of its stakeholders. Role-based access control is implemented where each user's access to the system is limited by the role they are assigned with. Thus, patients' information is only made viewable to those authorized for it. This will lower the chance of highly private progress record information being unnecessarily seen and disseminated.

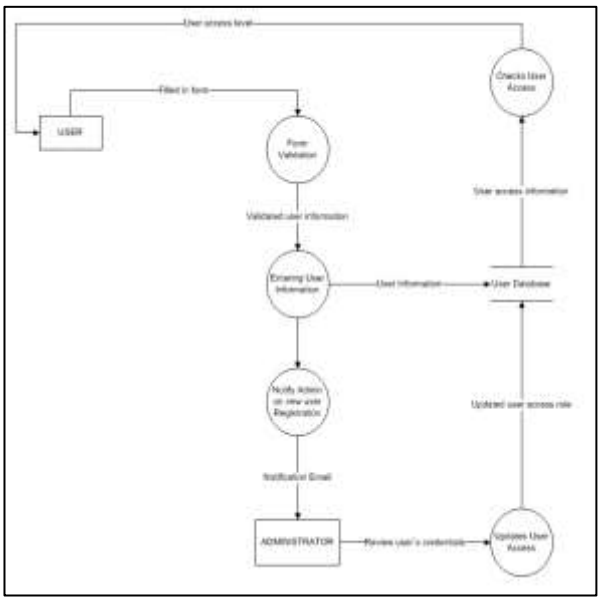

Figure 1. User registration and administrator assigning role to user

To satisfy the conditions of "asking for permission" and also "purpose specification", input from patient regarding their permission on the usage of their personal information is required and designed into the system. This informed consent section will calculate the document's access based on the agreement given by the patient.

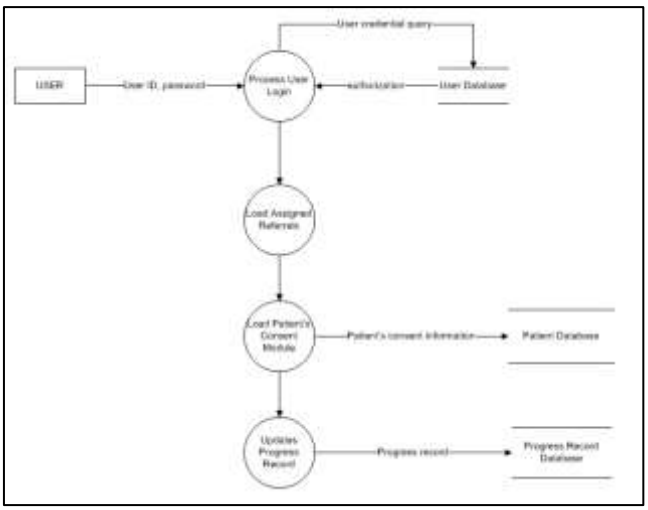

Figure 2. Recording patient's consent on personal information usage

Previous file-based system allows attending physicians and psychologist to share their thoughts by writing in the patient's file. This feature is preserved in the computerized system, but access are given to only selected psychiatrists and even then there are still information that can be keep only between the psychologist and patients by using private personal notes and private upload of images.

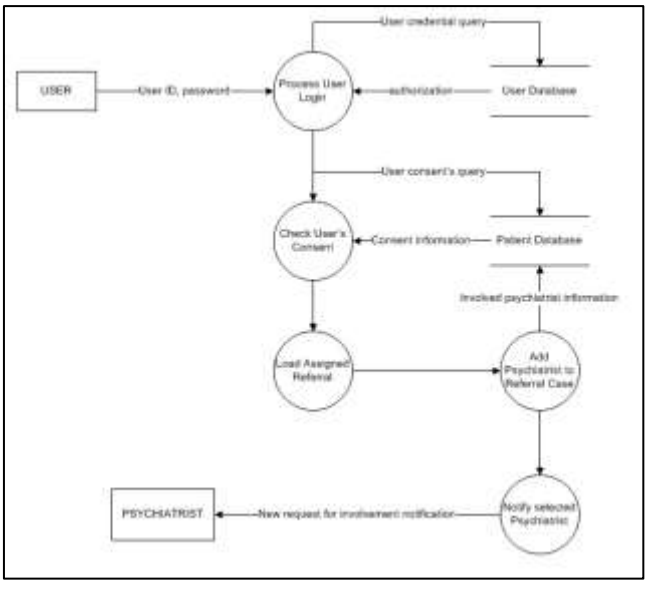

Figure 3. Assigning psychiatrist to a case

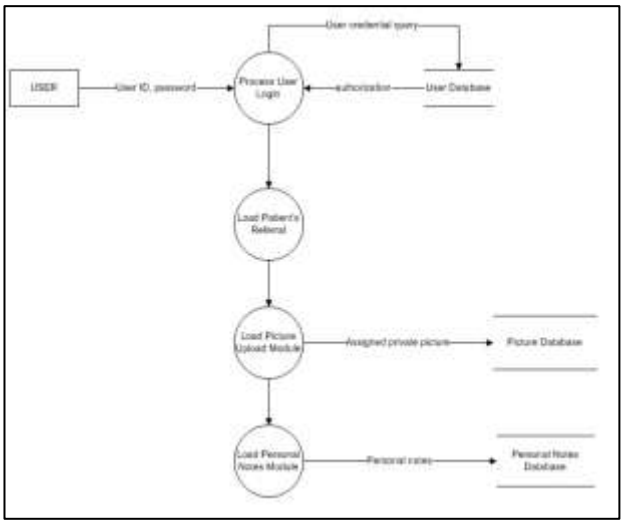

Figure 4. Uploading private picture and updating personal notes

VII CONCLUSION

Failure to address human values is one of the reasons of failure in information system. Values such as privacy should be in consideration before and during the design phase of a system. Islamic sources and tradition supports and extend moral values. Islamic values are not values that are in oppose of human values but they may be difference in execution. Privacy is such value where there are additional requirement in Islam on how privacy conditions can be satisfied. The study draws definition of privacy from Islamic and mainstream definitions. It then uses the techniques from Value Sensitive Design to develop system for Psychology Clinic Information System to respond for the privacy concerns arising from the usage of current file-based system it used. The developed system helps in keeping patients' information confidential bringing the highest concern in the highly confidential psychology progress note.

ACKNOWLEDGMENT

I would like to thank Dr. Azizah Othman from the Psychiatric Department of Hospital Universiti Sains Malaysia for her agreement and invaluable help in doing this research.

REFERENCES

ACM code of ethics and professional conduct. (1992). *Commun. ACM*, from http://www.acm.org/about/code-of-ethics

Association, A. P. (1993). Record keeping guidelines. *American Psychologist, 48*(9), 984-986.

Borning, A., Friedman, B., & Kahn, P. (2004). *Designing for human values in an urban simulation system: Value sensitive design and participatory design.* Paper presented at the Eighth Biennial Participatory Design Conference, Toronto, Canada.

Brey, P. (2000). Disclosive computer ethics. *ACM SIGCAS Computers and Society, 30*(4), 10-16.

Chapman, C. (2006). *Fundamental Ethics in Information Systems.* Paper presented at the 39th International Conference on System Sciences, Hawaii.

Fleurbaey, M., & Maniquet, F. (1997). Utilitarianism versus fairness in welfare economics.

Friedman, B., Peter H. Kahn, J., & Borning, A. (2002). *Value Sensitive Design: Theory and Methods*: University of Washington.

Kamali, M. H. (2008). *The Right to Life, Security, Privacy and Ownership in Islam*: The Islamic Texts Society Cambridge.

Mamat, M. N. (2008). *Dimensi Dunia ICT Islam - Menyelusuri Perspektif Etika dan Sosial*: Pusat Penerbitan Universiti (UPENA) Universiti Teknologi MARA.

Mason, R. O. (1986). Four ethical issues of the information age. *Mis Quarterly*, 5-12.

OECD. (2003). *Privacy Online: OECD Guidance on Policy and Practice*.

Padela, A. I., & del Pozo, P. R. (2011). Muslim patients and cross-gender interactions in medicine: an Islamic bioethical perspective. *Journal of Medical Ethics, 37*(1), 40.

Patil, S., & Kobsa, A. (2009). Privacy Considerations in Awareness Systems: Designing with Privacy in Mind. *Awareness Systems*, 187-206.

privacy. (2012). *Merriam-Webster.com* Retrieved 16th February 2012, from http://www.merriam-webster.com/dictionary/privacy

Velasquez, M., Andre, C., Shanks, T., & Meyer, M. (1996). Thinking ethically. *A Framework for Moral Decision Making*.

Yu, E., & Cysneiros, L. (2002). *Designing for privacy and other competing requirements*.

The Holy Qur'an: Text, Translation and Commentary Trans. Abdullah Yusuf Ali