RESEARCH ARTICLE OPEN ACCESS

Using PRE-GOV for Preserving Privacy: An Empirical Case Study

Haya Almagwashi*
*(Information Systems Department, King Abdulaziz University/Faculty of Computer and Information Technology Jeddah, SA
Email: halmagwashi@kau.edu.sa)

----------**********----------

Abstract:

This paper presents an empirical case study of applying PRE-EGOV privacy framework on a set of e-government services provided by Edu Portal. PRE_EGOV was developed in previous work and in this paper, weaim to apply the framework on a real-world case study to test its applicability usefulness. PRE-EGOV framework was used in identifying the privacy requirements and in designing privacy-friendly e-government services that preserve privacy and provide the users of these services with a tool to control access to their personal information. The application of the framework was successful and the evaluation of its usefulness and acceptance were positive. However, generalizing these results will need longterm research and applying it in many case studies in different countries.

Keywords—privacy, requirements, e-government services, data ownership.

----------**********----------

I. INTRODUCTION

Preserving privacy when providing e-services in general and e-government services has been a subject to many researches.

The PRE_EGOV framework presented in [1] provided processes that helps in theelicitationof the privacy requirementsand the designing of the e-service. It incorporates the concept of Privacy-By-Design while considering environmental factors that affect the identification of these services.

The application of the PRE_EGOV framework [1] is part of evaluating its usability as the framework needs to be applied to different case studies from countries with differences in the social, cultural and political environment to demonstrate its applicability and generality. Then after the application of the framework, the usefulness of the framework can be evaluated using a set of semi-structured interviews with relevant stakeholders to determine the usefulness and acceptance of the framework from different perspectives. However, this was faced with serious obstacles as it needed several agreements to be provided with access to information that some governments consider as classified. Over a long period, we had one government agency who agreed to cooperate and apply the framework on one of the existing e-services provided by this government agency. The results were so promising, and we would like to encourage other researchers and government agencies to consider the application of this framework to e-government services to verify its generality.

This paper presents details of the application of PRE_EGOV on the selected case study, and details of the usefulness evaluation based on the framework's application. An overview of the case study is presented in section 2, while details of the application of the framework provided in section 3. Section 4 present results of the usefulness evaluation and section 5 provide the conclusion.

II. EDUPORTAL SERVICES: AN OVERVIEW

EduPortal Services is an e-government portal which provides all the services that a sponsored student from country B might need in interaction with the government when he/she is studying abroad. The services of EduPortal vary from a simple download of official forms and applications to the submission of financial payment requests and scholarship extensions. The services are used by thousands of students from Country B studying abroad in many countries around the world. All EduPortal services are provided online and some services require the sharing of the students' data between different government agencies such as the ministry of education (MoE), Ministry of Internal Affairs, Ministry of Foreign Affairs, and government agencies in the country where the student study. EduPortal Services provides a large range of e-services that serve various student needs when studying aboard. The workflow of the EduPortal services is illustrated in Fig 1.

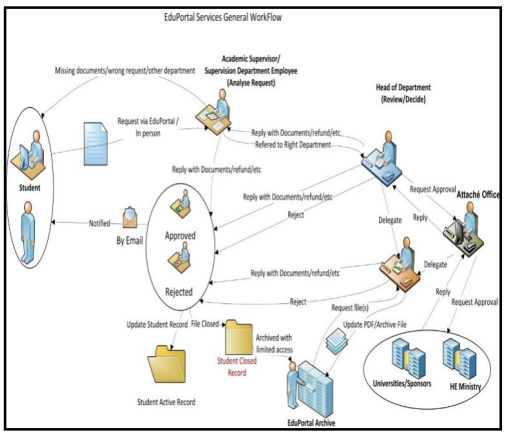

Fig 1 A general workflow for a service in EduPortal

For applying the framework in this case study, the following services were selected: (1) Update Electronic file including Update personal information and Update Contact information (2) Enquiry Request. (3) Scholarship Extension Request.

These services were selected based on the extent the service uses sensitive user data which is shared with other departments. The Update Electronic file service involves uploading personal information and confidential files which need protection and use only when needed. The Enquiry Request is general and involves different levels of data sharing between different government departments while the Scholarship Extension Request is rich in details and involves sharing specific data between different government departments and beyond with other government agencies and third parties.EduPortal system consists of different integrated applications that been developed overtime and accessed by the users via a unified interface and according to their privileges. These are: (1) the Educational services which deals with all services relevant to the student study from the start of the registration to the end via graduation or any other end,(2) the Financial services which deal with all the financial request either the student monthly payments or payments for study fees or other expenses , the Archive which add all paper work related to the student to a large pdf file, and finally the Request workflow (which lists all the request made and their current status.

A. Student Record Structure

The student record has two main parts:

1. **The Data File:** This is stored in a DB which includes all student information and a history of all requests or actions performed on the student record. This record is accessed by all EduPortal portal applications and can be viewed by an employee from any department. However, any updates to the student record are due to data entered using the provided services. This data can be entered by the student, for example, when updating contact information or by an employee in the office as part of a response to a request made by the student.
2. **The PDF File:** This replaces an old physical paper file and contains any document about the student, since the student started and opened a file in the government office. These documents can be provided by the student, his sponsor, the university providing the study course or by the government office employees. It is segmented into sections, such as financial and educational and a document is added to the relevant section. The file documents are sorted by date of entry to ease access to a required document.

B. Student Record Structure

Access rights to an active student record are role-based. For example, all employees in the department responsible for postgraduate students sponsored by a university can view the records of students supervised by that department, and are not allowed to access records of students of other departments with a few exceptions given to some employees who have senior roles, such as the head of a supervision department who needs to view a student record which is moving to another department (e.g. a student completed a bachelor degree and starting a masters). When an employee is processing a request from a student because of his role, he can view the whole record of the student (Data and PDF parts). However, he cannot change, add or update any parts of the record unless processing a request made by a student and responding to the request initiates the change. Each action performed on a student record due to a request is logged under the request information in the data file section in the student record with information about the employee who performed the action. When a student record is closed (e.g. a student has finished his scholarship and graduated) the record is marked as archived and access rights to this record become more limited. Access rights to view archived files are limited to some senior roles such as the attaché or the deputy attaché. Access to view all student records (active or archived) for reporting or general analysis purposes is limited to a few senior roles (e.g. e-services manager).Also, no student record can be changed altered or updated without a request initiated by the student or an employee in the government office on behalf of the student and the student is always notified about such requests.

III. APPLYING PRE_EGOV FRAMEWORK

PRE_EGOV framework has three main stages: Preliminary, Requirements Elicitation Analysis, and Design. The framework also has three main supporting elements. These are the Environmental factors influence management, the Regulations, laws and policies compliance management, and Privacy awareness supporting element. These supporting elements are considered in each phase when applying the framework and relevant questions are asked during each phase in the framework. However, a discussion of these supporting elements will be provided after presenting the main phases of the framework. In the case study, the framework is applied on selected services in EduPortal namely: Update Personal and Contact Information; Enquiry Request; and Scholarship Extension Request.

A. *Preliminary Phase*

This phase required input from the preliminary interviews with relevant stakeholders which have been done in two rounds to identify their expectations and needs and establish agreement on the definitions proposed by the framework. The rounds were done before and during the application of the proposed framework. The aim of the first round of interviews was to understand the current system and the processes of the selected services and identify relevant stakeholders. It also aims to get stakeholders' views on the privacy issues in the current system and to identify their privacy requirements, their expectations and needs when using the selected services. Then a second round of interviews was performed during the application of the framework to confirm the requirements and resolve any conflicts. The selected sample for the interviews included ten users (four male, six female) with different backgrounds and ages, three service provider representatives, two developers and one government representative. The identified preliminary stage tasks were applied as follows:

1) Expectations and Needs Identification:

- **Stakeholder Identification:**

a. **Users:** Students age 18 and over, male and female, studying various degrees, such as English language programs, bachelor's degree, diplomas, master degrees, PhD degrees, and post-doctoral degrees. It is important to clarify that throughout this chapter, we refer to data subject users and when the reference is to other types of users who are using the EduPortal system, and this should be clarified and referred to as non-data subject users. Also, the employees in the services providers' stakeholder category, use the system to provide the services (e.g. process students' requests), however, they are considered as non-data subject users and by users we mainly mean data subject users.

b. **Government body representatives:** Higher Education Ministry who provide EduPortal services and E-government strategic planning agency who approve new services or changes in the provided services.

c. **E-government services Provider(s):** Government Office(s) (mainly embassy(ies)) in foreign countries where students study, MoE who take part in processing and approving some of the services, student sponsor representatives who take part in processing and approving some of the services and employees in government offices who are processing users' information (data subject users) to provide EduPortal services.

d. **Developers of e-government services**: A government owned company who design and implement most of the e-government services, developers from the MoE.

- **Stakeholders Expectations and Needs:**

In this step, for each service, the expectations and needs with respect to preserving privacy when using the services were gathered by following the steps detailed in [1] These are:

1.Select a representative sample of identified stakeholders.

2.Identify the expectations and needs of relevant stakeholders.

3.Review stakeholders' requirements and resolve possible conflicts between the identified requirements.

A sample of ten students using the system was selected as representative of the user category. The aim was to select students with different age, social background and studying different degrees. The selection involved 4 male students and 6 female students who study different courses (undergraduate and post graduate) - some married and others single. The sample for the other stakeholders' categories included, one government body representative, three service providers including a representative of the MoE and two employees who work in other government departments in the foreign country and deal with student requests made through EduPortal in two different departments, and two developers, one who works for MoE and the other an independent developer working on a similar system. It is believed that the sample is representative of the stakeholder categories as the researcher made every possible effort to select the sample carefully so that it represents student and other stakeholder categories and covers as many varieties in their needs and expectations as possible.

The next step was to identify the expectations and needs of the identified stakeholders. One-to-one semi-structured interviews were used. The identified expectations and needs were documented for each service and prioritised according to their importance to the stakeholders. These expectations and needs were formulated as privacy requirements and sorted by priority from the perspective of the users who are the data subject are:

1. The users of EduPortal services (data subject users) need to have full control over sensitive information about them.
2. The users (data subject users) need to know who is viewing information about them, what information is viewed, and what is the purpose of viewing that information?
3. Users (data subject users) expect the employee who is processing the requested service to be able to view only information needed and relevant to that service.
4. Sensitive files and documents about the user (data subject users) should be encrypted and accessed only when needed and by limited employees.
5. Users (data subject users) should be notified of any override to the privacy settings set by them over information about them.
6. Employees' identities (who are users of the system but not a data subject of the processed data) should be protected and not viewed by users (data subject users) unless this is needed (by services provider and/or government representative perspectives).
7. There should be an option for overriding privacy settings applied by the user (data subject users) by

senior employees in EduPortal system in emergency cases (by services provider and/or government representative perspectives).

- **Review requirements and resolve possible conflicts**

For each service, the privacy requirements were reviewed with the stakeholders and identified conflicts and proposed resolutions were negotiated.

2) ***Data Classification:*** The following data classifications were agreed by all stakeholders: Restricted Data, Sensitive Data, Private Data, and Public Data. The definitions of these classifications were based on the definitions provided in [1].

3) ***Ownership Rights Definitions:*** The ownership rights definitions suggested by the PRE_EGOV framework [1]were used and agreed by all stakeholders with a slight change to the Totally Owned definition, namely "the right to delete the information owned" was omitted from the definition and replaced by a hide option that allow the user to prevent access to the data or viewing it but not deleting it.

4) ***Levels of Control Definitions:*** The following definitions of Levels of Control based on [1] were agreed by all stakeholders as follows: (1) **Full Control**: The user is given the right to allow or prevent any access right to a piece of information i.e. allow or prevent view, change or share of the information. (2) **Partial Control**: The user is given the right to allow or prevent the viewing, sharing of a piece of information. (3) **No Control:** The user does not have any right to allow or prevent access rights to a piece of information. An important requirement is providing an option to override the privacy settings applied by the user. This was introduced to give full control to the service provider in emergency cases.

5) ***Data Types Mapping:*** Table 1showsexamples of the data mapping from the user data used to explain the relation between ownership rights and levels of control and the data classification.

TABLE 1 EXAMPLES OF PRIVACY SETTINGS OVER USER'S INFORMATION

Data	Privacy Settings	Comments
National ID	{Private, Partially Owned, Partial Control}	The user can view and change the data through a request, while controlling the viewing of the data and changing of the data by others. The system can still use the data for verification of the identity.
Marital status	{Restricted, Totally Owned, Full Control}	The user can view, edit and hide the data and have full control on allowing or preventing the viewing, editing of the data by any one.
Passport ID	{Private ,Partial ly Owned, No Control }	The user can view and change the data through a request but has no control on allowing or preventing access rights to the data. However, the user should know who is viewing the data and when the data is viewed and by whom.
Address	{Sensitive, Totally Owned, Partial Control}	The user can view, edit and hide the data and have partial control on allowing or preventing the viewing, editing of the data.
Mobile phones	{Totally Owned, Full Control, Sensitive}	The user can view, edit and hide the data and have full control on allowing or preventing the viewing, editing of the data by any one.
Email	{Private ,Partial ly Owned, Partial Control}	The user can view, edit the data and have partial control on allowing or preventing the viewing, editing of the data.

B. Requirements Elicitation Phase:

1) ***Data Classifications Identification:*** Information about the user that is needed in processing and providing the selected services was analysed and classified to the data types defined in the preliminary phase according to the identified expectations and needs of the user. The classification is shown inTable 2.

TABLE 2 AGREED DATA CLASSIFICATION

Data	Classification
Personal Details	
[Name, Gender]	(Public)
[National ID number, place of birth]	(Sensitive), Default (Private)
[Marital status]	(Restricted), Default (Sensitive)
[Birth date]	(Restricted), Default (Sensitive)
[Relatives names]	(Private), Default (Public)
[Relatives mobile numbers]	(Sensitive), Default (Private)
Bank details] (Sensitive), Default (Private)	(Sensitive), Default (Private)
[Passport ID, Date of issue, Place of Issue]	(Private), Default (Public)
[Passport Expiry date]	(Public)
[Visa number, Date of issue, Place of Issue]	(Private), Default (Public)
[Visa Expiry date]	(Public)
[Sensitive personal files (e.g. personal pictures, copies of the passport, or any other personal identifiable documents, marriage or divorce certificates)]	(Sensitive), Default (Private). Accessed only when the service totally depends on the information in these files)
[Official files (e.g. decisions on sponsorship, government letters, etc.)	(Private), Default (Private)
Contact Details	
[Mobile numbers]	(Restricted), Default (Sensitive)
[email]	(Private), Default (Public)
[Qualifications details]	(Public)
[Education study details]	(Public)

2) Privacy and Security Requirements Elicitation

In this task, first a risk analysis relevant to the privacy of the users' information was performed based on interviews with the stakeholders and the risks identified by the service provider. Table 3 summarises identified risks relevant to the services, their potential impact and likelihood, and suggests mitigation safeguards for these risks. The impact levels are low, moderate, and high, and describe the level of the adverse

effect on organizational operations, organizational assets, or individuals in the case of the loss of confidentiality, integrity, or availability of the information as defined by NIST [2] and OEDC [3].

TABLE 3 IDENTIFIED PRIVACY RISKS AND SUGGESTED MITIGATION

Rank	Identified Risk	Potential Impact /Likelihood	Suggested Mitigation Safeguards
1	Disclosure of personal information about the user	High/High	Access rights are limited to user's sensitive personal information
2	Corruption/changes of information about the user	High/High	Changes to users' information are made through processing relevant services.
3	Destruction of information about the user	High/High	No delete option /backup data regularly
4	Unauthorised access to users' information	High/Moderate	Stronger authentication measures/log access
5	Black mailing/threats to users as a result of disclosure/theft of all or part of user information	High/Moderate	Limited access to user information/only when needed
6	Disclosure of information about other people related to the student	High/Moderate	Limited access to relatives' information
7	Unauthorised access to the system	High/Moderate	Strong secure authentication measures /system log
8	Denial Of Service	Moderate/Low	Provide alternative routes for a service,
9	Bias on decisions related to other services as a result of viewing information not needed for the service	Low/Low	Employee should view only needed information for the service

- **Privacy requirements:**

Based on the outcome of the interviews and the identified risks on user information, the following privacy requirements were identified for the selected services. 25 general Privacy Requirements (PR) were identified for all the selected services:

PR1. The system should view only the needed information for the processing of the service.

PR2. The system should allow the user to decide on the information about them which is sensitive.

PR3. The system should allow users to have full control and the ability to limit access to their sensitive information.

PR4. The system should encrypt sensitive files about the user (currently included in the pdf file of the student records).

PR5. The system should provide protection and limit access rights to sections of the student record with sensitive information.

PR6. The system should allow the user to know who accessed his/her personal information, what information was accessed, when it was accessed and for what purpose.

PR7. The system should provide privacy awareness alerts and messages to the user and the employees to explain the impact of their actions on user's privacy when initiating or processing a request where appropriate.

PR8. The system should provide an option to override any privacy settings in emergency cases so that senior roles can access any user information which is needed.

PR9. The system should notify a user when any override occurs to the privacy settings applied by the user.

PR10. The system should consider contact information as sensitive information and limit access to this information.

PR11. The system should notify the user of any changes made to his/her information.

PR12. The system should not allow automatic delegation of processing a user's sensitive information without the user's consent.

PR13. The username used by the user to login to the system should not be a personal identifiable piece of information (e.g. National Identity Number, emails).

PR14. The user should be notified when any disclosure of information about him occurs, (either by accident or by an intended breach of the system or the user account).

PR15. All the system's users should be made aware of relevant privacy policies, regulations and legislations applied or being introduced.

PR16. The system should protect the identities of employees providing a service, by providing an Employee reference number for each employee.

PR17. The system should log the Employee reference number with each process performed on the user's information.

PR18. The identity of the employee with a particular employee reference number should only be known to people with senior roles in the government office.

PR19. The system should ensure that privacy preferences are applied as long as the information exists.

PR20. The system should apply stronger authentication methods to verify the user's identity when the user performs changes to his/her privacy preferences on information.

PR21. The system should limit access rights to backups of user information only to people with a senior role and the user should be notified about this.

PR22. General reports produced by the system should consider a user's privacy preferences.

PR23. The system should provide an option of private enquiry for enquiries that involve providing sensitive information and files.

PR24. Private enquiries should be processed by as few people as possible and only if needed.

PR25. The system should give access to sensitive information or supporting files included in a request, only to employees who are processing a scholarship extension request at a different government agency and only when it is needed for decision making according to their roles.

- **Security requirements:**

The Security Requirements (SRs) for the selected services were identified as:

SR1. The system should authenticate the user by username (National Identity number) and a strong password.

SR2. When the user forgets the password, the system should offer the user a way to recover the password (Currently by sending the password to the user's email registered in the system).

SR3. After three fail attempts at login, the user account is locked and can be opened only by answering a pre-set set of challenging questions.

SR4. User information cannot be changed unless it is by one of the system services.

SR5. Sensitive personal information about the user should be protected by high security measures.

SR6. Personal information and contact information should always be up-to-date

SR7. Changes in personal information should be supported by relevant evidence documents to validate the accuracy of the changes before approval. For example, a change in passport information requires providing a copy of the new passport.

SR8. Changes in personal information are only done by request to update personal information.

SR9. Changes in contact information are done by a request to update contact information.

SR10. Contact information should be considered as sensitive information and protected by access rights.

SR11. Any personal official files provided to support the request should be considered sensitive and protected by strong security measures.

SR12. Personal information and files should be accessed only when needed.

- **Additional identified requirements:**

Some additional Functional Requirements (FR) which relate to privacy and security were identified:

FR1. FR1. The system should give meaningful names for uploaded files by the users.

FR2. When the user is asked to support a requested service with an official document, the system should provide the user with a list of previous uploaded files to allow the user to select the file if it already exists in the system to avoid redundancy by uploading the same file many times.

FR3. The privacy preferences set by the user should not prevent the user from accessing the requested service.

FR4. The user should be notified if the current privacy preferences will affect processing the requested service or delay the response to that request.

FR5. The default privacy preference settings should support protecting the user's privacy.

FR6. The system should allow users to view the workflow of the request and the notes and alerts that concern them, and the expected time of processing of the request at each point as appropriate.

FR7. The system should allow an employee to view relevant alerts about the student related to the requested service.

3) Ownership Rights and Levels of Control Identifications

In this step, the desired ownership rights and levels of control over information about the user were identified. The users would like to have full ownership rights on sensitive information about them or their relatives and would also like to have full control on such information. However, the service providers and government have some restrictions on giving full control to some of this information. Based on the previous identified privacy and security requirements and desired data classifications agreed by stakeholders, ownership rights and levels of control over pieces of information were assigned to each data type as described in the next section.

4) Ownership Rights and Levels of Control Assignment

The assigned ownership rights and levels of controls agreed by relevant stakeholders are presented in Table 4. These setting can b controlled by the user as privacy settings in the form.

TABLE 4 OWNERSHIP RIGHTS AND LEVELS OF CONTROL ASSIGNMENTS

Data	Privacy Settings	Comments
National ID	{Private, Partially Owned, Partial Control}	The user can view and change the data through a request, while controlling the viewing of the data and changing of the data by others. The system can still use the data for verification of the identity.
Marital status	{Restricted, Totally Owned, Full Control}	The user can view, edit and hide the data and have full control on allowing or preventing the viewing, editing of the data by any one.
Passport ID	{Private ,Partially Owned, No Control}	The user can view and change the data through a request but have no control on allowing or preventing access rights to the data. However, the user should know who is viewing the data and when the data is viewed and by whom.
Address	{Sensitive, Totally Owned, Partial Control}	The user can view, edit and hide the data and have partial control on allowing or preventing the viewing, editing of the data.
Mobile phones	{Totally Owned, Full Control, Sensitive}	The user can view, edit and hide the data and have full control on allowing or preventing the viewing, editing of the data by any one.
Email	{Private, Partially Owned, Partial Control}	The user can view, edit the data and have partial control on allowing or preventing the viewing, editing of the data.

C. Design Phase:

1) Rules and Controls Presentation

The main requirements regarding the presentation of the levels of control were identified by considering the identified expectations and needs in the previous phases and by considering the different capabilities of the users. The identified Privacy Design Requirements (PDRs) are:

PDR1. The system should show the privacy settings in the main page.

PDR2. The system should allow one time setting of privacy preferences for all services.

PDR3. The system should provide appropriate privacy alerts when a user changes the level of sensitivity of a piece of information.

PDR4. Privacy alerts and help messages should be provided in a simple language that can be understood by all types of users.

PDR5. Default privacy settings should be explained when the user first uses the system.

PDR6. Employee should have alerts each time he/she logs in to the system about currently applied privacy laws and should acknowledge reading it.

PDR7. A log file should be kept for all transactions made on a user's data while the user record is active.

PDR8. Each log entry should describe the action performed, on what data, when and by whom and who initiates it. For example, if the request was initiated by a user using EduPortal, then the user (identity number) ID and IP address should be entered in the log file. However if the employee is that one processing the request, then the employee reference number should be entered.

PDR9. Access to the student record (PDF file) should be protected by passwords and sections with restricted data should be encrypted.

PDR10. Log files should be protected by high security measures to prevent any tampering with the logged data.

PDR11. A onetime password is required when changing the privacy preferences settings; this password is sent to the registered mobile number of the user.

PDR12. Registering or changing the mobile number of the user should be in person or via the site and answering a security question.

PDR13. A timeout should be set to 5 minutes with no activity on the privacy settings pages.

When the requirements are implemented in the system, Privacy Enhancing Technologies (PET) can be used in the implementation to satisfy these requirements. Examples of PETs meeting these are: IBM's Secure Perspective software which allows organisations to create and manage enforceable security policies using natural language [4], Hewlett Packard's Openview Select Identity which enables organisations to manage users and their privileges [5], Privacy meta data use is suggested for tagging information about the user with relevant metadata that defines access rights to the data, any related conditions on the use of the data and whether the user's consent is required before sharing the data with third parties [4] and any other technology can be used which satisfies the identified privacy requirements.

2) Rules and Control Deployment

Based on the identified requirements, assigned ownership rights and levels of control identified in the second phase, a prototype which satisfies the identified privacy requirements for the selected services was developed. The screens of the prototype were developed as mock-up prototype screens.The resulting prototype demonstrates how students using EduPortal can set their privacy preferences on the information about them and how the EduPortal system is affected by these privacy settings. Snapshots of the resulting prototype are presented in the provided example scenario which show screens related to: Privacy preferences settings, Data sensitivity settings, Data control level settings and Employee interface for a selected service (Educational Enquiry Request). The complete prototype for the selected services werepresented to stakeholders for evaluation purpose as discussed in the following section. These screens were explained and viewed to relevant stakeholders so that they can provide feedback and possible enhancements which are considered in the development of the services. An actual implementation of the proposed solution within the e-government service is not included as it is out of the scope of this paper and required integration with the current system of EduPortal Services and were not revealed to preserve the confidentiality of the government agency.

- **Example scenario:**

When the student logs in to the system, a Privacy Preference Setting screen appears with three choices. When the student selects any of the options, he/she will be asked to enter a onetime password to get access to the selected privacy preferences settings choice. The Privacy Preferences Settings options are: 1) Data Sensitivity Settings; 2) Files Sensitivity Settings; and 3) Data control Levels Settings.If the student selects the Data Sensitivity Settings option, the student can view and change the sensitivity settings (data type) assigned to a piece of information as appropriate (**Fig 2**). If the user does not have the required ownership right for a data type, this data type will appear as disabled

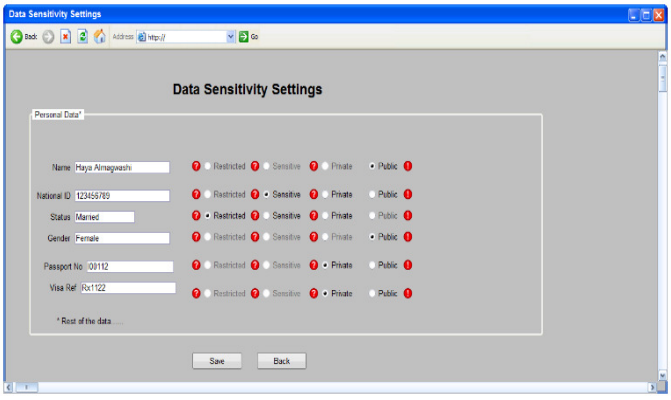

Fig 2:Data Sensitivity Settings

The red question marks provide messages to explain the effect of selecting the corresponding data type. These messages appear when the user clicks on a mark (**Fig 3**).

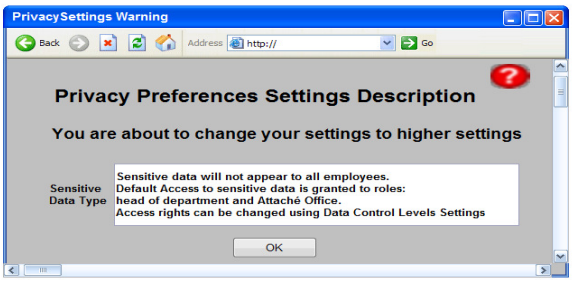

Fig 3:Privacy Preferences Settings

The option File Sensitivity Setting allows the student to view and change the sensitivity setting (data type) attached to a document that is included in the student record (**Fig 4**).

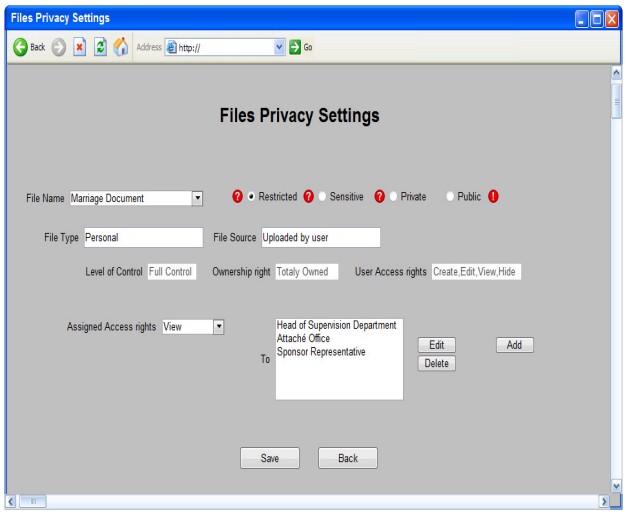

Fig 4:File Sensitivity Settings

The option Data Control Level Setting allows the student to change the access rights to each piece of information according to the assigned ownership rights and levels of control of that piece of information. According to the assigned ownership rights and levels of control, the user can control access rights to this information or leave it to the default settings. In the example, the student has Totally Owned ownership right and Full control on this piece of information. Thus, the student has all access rights and can control also access to that information.

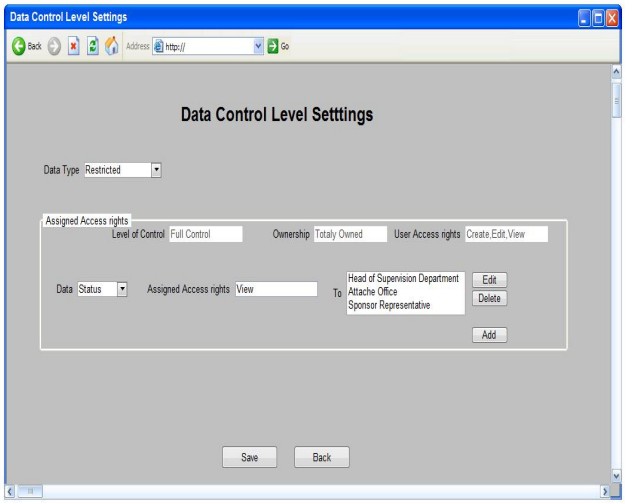

Fig 5 , the user gave the view access right to the roles of Head ofsupervision department, Attaché Office and Sponsor Representative. If the user limits the access rights to this information to none or very few people, in a way that will affect his/her ability to request a service, appropriate alert message will appear.

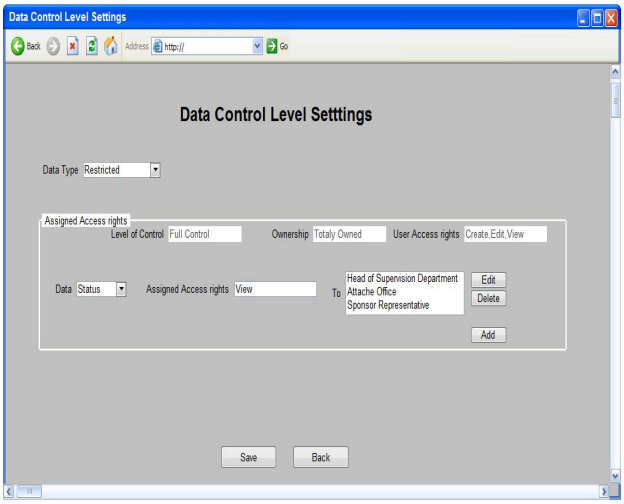

Fig 5: Data Control Level Settings for Restricted Data (Marital Status)

The example in**Fig 6** is about an employee processing an Enquiry request (Educational). Thesettings applied by the user affected the employee's ability to view some of informationand only relevant information to the request can be viewed.

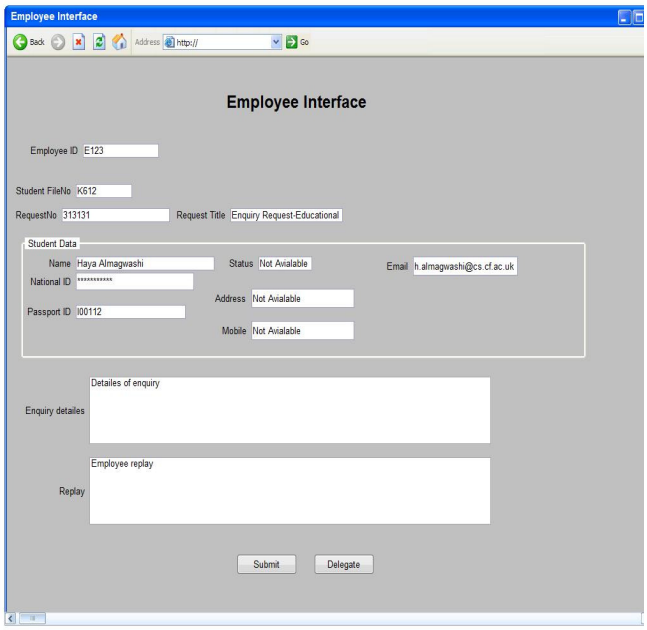

Fig 6:Employee Interface for an enquiry request

3) *Environmental Factors Influence Management*

Environmental factors have been identified and their impact on the identification of privacy requirements was considered in the deployment of all the phases of the framework.

The identified factors are:

- The government has signed an international agreement that obliges all agreeing parties to have privacy regulations and laws in place by 2016 and to comply with OECD privacy guidelines [3], [Political, Legal].
- The government are open to different opinions from stakeholders, however, full control on the data used in e-government services should be in the hands of the system owner (the government),[Political].
- Users of the EduPortal system have at least a secondary school level of education, which means they are able to understand how to use the services, [Social].
- All students have access to the internet. Kiosks are provided in foreign government offices. Also, students can request a service in person at a government office, [Social].
- No user can use the EduPortal services on behalf of another user, [Political].
- Gender difference should be considered when identifying privacy requirements, [Social].
- Increasing a user's trust should be considered, [Cultural, Political].

4) *Regulations, Laws and Policies Compliance Management*

A privacy law was introduced and applied, at the beginning of 2013in country B, which states that any individual or organisation that seeks to collect unauthorised documents or confidential information by any means will face a sentence of up to 10 years in prison and a large money penalty. This cannot be referenced for confidentiality agreement of the case study.

5) *Privacy Awareness*

Privacy awareness programs should be provided for both students and employees. The students' privacy awareness program can be given as part of the induction workshop where they learn about using the EduPortal system and for the employees as part of their training programs. In addition, the EduPortal services system will display warning messages for users, when they change their data privacy settings to a lower sensitive level. Alerts about relevant privacy policies also will be displayed to employees as appropriate.

IV. PRE_EGOV USEFULNESS EVALUATION IN EDUPORTAL

The evaluation of the usefulness of PRE_EGOV frameworkinvolved applying the framework in the EduPortal Services case study then conducting semi-structured interviews with relevant stakeholders to evaluate the usefulness of the proposed framework. The application of PRE_EGOV in the EduPortal case study required three rounds of interviews with a selected sample of relevant stakeholders as described in previous sections. The aim of these interviews was to engage stakeholders in the steps of applying the framework and identifying privacy requirement.

Another round of interviews was conducted to evaluate the usefulness of applying the framework in EduPortal case study. The semi-structured interviews were conducted after applying the PRE_EGOV framework in the selected services of EduPortal. Each interview lasted about 90 minutes and in the first 20 minutes the researcher briefly presented the proposed framework and illustrated the framework steps followed to identify the privacy requirements and assign the ownership rights and levels of control to the user information. Prototype screen shots for different scenarios were used to demonstrate how the application of the framework will enable a user to have control over their privacy while taking account of the security requirements of the provided services. The presentation was followed by asking general open questions. The questions covered what interviewees thought about the proposed framework in general, if the steps of applying the framework were in general clear and whether the application of the framework will increase their trust in using EduPortal services. In addition, interviewees were asked about the identified privacy requirements and assigned ownership rights and levels of control. Two hand-outs of the definitions and the identified privacy requirements, resulting from the application in the preliminary phase, were handed to the interviewees. Hand-out 1 showed the definitions proposed by the framework for the ownership rights and levels of controls and data types illustrated with examples, while the second hand-out had the forms used for identifying privacy requirements and the agreed resolution for identified conflicts. The interviews were followed by providing a set of questions listed in a short

questionnaire which each interviewee was asked to answer and complete. The sample in the evaluation round of interviews included the same sample of stakeholders who were interviewed during the application of the framework in the EduPortal case study except for two new interviewees from the user category. The sample included: six (Users). Also, the sample included three services provider representatives (SPs) , and two developers, one of them involved in the development of EduPortal services and another independent developer is familiar with the development of e-government services (Devs). In addition, a government body representative [GR] was interviewed. It is believed that the selected sample is representative of the stakeholders, since the user sample was selected carefully to cover different groups of users both male and female, and students with different social circumstances and levels of study, also the number of interviewees from each stakeholder category represents an approximate percentage of their actual proportion in relation to the provision and use of the EduPortal services.

A. Results Analysis

In the evaluation interviews, the aim was to identify privacy issues that users and other relevant stakeholders had with the current system and get their feedback on the proposed framework to see if the proposed framework improved the preservation of privacy and tackled the identified issues in the current system.

1) Responses about the current system (EduPortal Services)

Based on the evaluation interviews, the main features that the users and other stakeholders liked about the current system were: 1) Quick response to requests, 2) Easy to use interface, and 3) Student's data can be changed only via requests initiated by the student. However, there was general agreement that the current system does not preserve the privacy of the users (students) and that any employee processing a student's request has access to all the student. These features were considered when applying the proposed framework and considered in the proposed solution to satisfy the requirements.

2) Responses about the application of PRE_EGOV in EduPortal

The application of the framework required three rounds of interviews and in total around 10 working days included applying the framework activities, conducting interviews, identifying privacy requirements, verifying the requirements with relevant stakeholders, and developing prototype screens. However, the arrangement for interviews took longer than expected and periods between responses between rounds of the interviews stretched up to three months with services providers and the government representative. Access to services providers' representatives and the government representative was a real obstacle due to their busy schedules; however, their feedbackwas very valuable. The main findings on the application of the proposed framework were:

- All interviewees agreed on the proposed definitions for ownership rights and levels of control and thought the definitions were clear and comprehensive.
- All interviewees agreed on the identified privacy requirements, and the suggestions for resolving identified conflicts and no additional requirements were identified.

The interviewees were shown a presentation about the steps of applying the framework in selected services of the EduPortal Services and screens of the prototype of the proposed solution resulting from the application of the framework. Next, the interviewees were asked about what they thought about the steps of the application of the framework and the resulting prototype. Their responses were:

- All interviewees from the user category liked the way that they had been consulted throughout the application of the framework and that the resulting requirements expressed their opinions. This was valued also by services provider representatives and the government representative, although they emphasised that the system owner (the government ministry of HE) should finalise and approve the privacy requirements to be satisfied by the system.
- The users in general thought the steps of applying the framework were clear, however, some users emphasised that providing examples to clarify the data types and the ownership rights and levels of control helped them to decide on what is important and sensitive to them). Services providers and the government representative also said that the steps of the application of the framework were easy to follow while both developers thought the framework is applicable.
- Most of the interviewees agreed that the willingness of the government to apply the framework would be a key factor in its successful implementation.

3) Responses about the features of the PRE_EGOV framework

The proposed framework's usefulness, acceptance and effect on increasing users' trust in using the EduPortal services were evaluated in the final interviews. The interviewees were asked if the application of the framework and the implementation of the proposed prototype resulting from the framework will increase their trust in using EduPortal Services. In addition, the proposed framework was evaluated against the criteria of the proposed solutions for preserving privacy in e-government derived from the developed in [1]. The criteria and additional questions about the interviewee agreement on usefulness, viability and acceptance of the proposed framework were included in the short questionnaire which was handed out at the end of the final evaluation interviews.

Regarding the question about whether the application of the proposed framework will increase users' trust in using the EduPortal services, all interviewees agreed that the application of the framework will increase users' trust in using EduPortal

services. A quote from a services provider representative interview is "I believe it will increase users' trust in EduPortal services and it will make them make less visits when they have sensitive issues (many students come to the government office when it is a personal matter to avoid uploading files in the service.)".

A summary of the responses indicating the percentage of total agreement is presented in Table 5.The responses show that there is general agreement between stakeholders on the usefulness and transparency of the proposed framework and that the framework considered the identified social and cultural factors. Most stakeholders agreed that the proposed framework is viable and easy to use, while a quarter of the stakeholders had no opinion on these two issues. Regarding the flexibility of the proposed framework, more than half of the stakeholders agreed that the proposed framework is flexible. Most users and the government representative agreed that the proposed system is flexible and considers dynamic changes in their needs. However, some users, the services provider representatives and one of the developers were cautious in their responses and chose no opinion.

TABLE 5: SUMMARY OF RESPONSES OF EVALUATING FEATURES PRE_EGOV

Criteria	All (12)
Usefulness	100%
Accepted by users	75%
Accepted by Services provider	25%
Is viable	83%
Easy to Use	75%
Transparent	100%
Flexible	58%
Meet identified security requirements	75%
Enforce Local relevant laws, policies	50%
Complies with relevant international standards	50%
Considers the impact of social and cultural	100%
Considers the impact of political factor	42%
Cost effective	25%

A services provider representative who disagreed about the flexibility of the framework explained his opinion as "Flexibility depends on the implementation, if the application is designed very well and the policies are applied well, the framework provides these requirements, you propose how it can be satisfied, however the way it is applied determines if the flexibility is satisfied, if the requirements defined are met, then the system is flexible ". Regarding agreement that the proposed framework will be acceptable to users; the responses showed that all users agreed that the proposed framework will be accepted by users of EduPortal.

However, the government representative, and a services provider representative who has an important role in the EduPortal Services, and the developer involved in the development of EduPortal services disagreed. Interestingly, most of the users were cautious on agreeing that the services provider will accept the proposed framework and chose no opinion, while one user disagreed. However, the government representative strongly agreed that the government will accept the proposed framework. This indicates a gap in the understanding of other stakeholders' opinions and mistrust between involved parties.

Users' responses showed a general agreement that the proposed framework has met the identified security requirements. Most of the services providers have also agreed. Regarding enforcement of local laws, most of the users stated that they do not know if there are any existing laws about privacy and chose no opinion, while the government representative, the developer from the government side and most of the services provider representatives agreed that the proposed framework considered the enforcement of local laws in the identified requirements. A similar response occurred for agreement on whether the framework complies with relevant international standards. All the services provider representatives, the government representative and the developer from the government side agreed that the proposed framework considered relevant international standards and guidelines. However, most of the users chose no opinion as they were not aware of the contents of these standards. The government representative agreed that the political point of view and impact was considered in the proposed framework while most of the users chose no opinion. Finally,a majority of the stakeholders gave no opinion on whether the proposed framework is cost effective or not. However, a general impression from the interviews was that there are some worries that it might cost time and money especially when applied in the existing services. However, the government representative agreed it could be cost effective in the long term and supported the application of the framework. Some additional feedback was given on the element of privacy awareness. The users liked the consideration of this in the prototype proposed by the framework.

In summary, there was positive feedback on the application of the framework and the results of its application. Some of the identified privacy requirements: PR11, PR14, PR15, PR23 and PR24 were listedas requirements for the updated version to the services which was due during the application of PRE_EGOV in the EduPortal Services. As a result, some changes in the provided services were made to satisfy these requirements. These are: a new option of private enquiry added to the types of enquiry in the Enquiry Request service with the process of this type of enquiry limited to the role of the head of the supervision department or higher roles; users would receive notification emails when their personal or contact details are changed; and emails about applied privacy policies and laws were sent to users of EduPortal.

B. Discussion

This section discusses the evaluation results in more details, the useability, usefulness and acceptance to the framework, the generality of the proposed framework, and possible limitations.

1) Findings

Careful observation of the application of the PRE_EGOV framework in the case study (EduPortal) suggests that the proposed framework is useable and can be applied easily in the context of e-government. It also showed that all stakeholders involved in the case study accepted the framework and thought its application will be useful in preserving privacy in e-government. In addition, the PRE_EGOV framework satisfies the criteria identified in [1] for a privacy framework.

2) Usability Evaluation

The usability of the framework i.e. the ease of use of the framework and the applicability of the framework were confirmed during the application of the framework in the case study. All the interviewees agreed that the framework is useable and can be applied to any e-government service. The interviewees were engaged in the application of the framework and the steps of the framework were explained to them in the initial and final interviews. All interviewees from the different stakeholder categories confirmed that the framework steps are clear and easy to follow. In addition, the viability of the proposed framework at an abstract level was supported by the survey results presented in Table 5. However, the willingness of a government to apply the proposed framework is a key factor in its successful implementation.

3) Usefulness and Acceptance Evaluation

The results of the survey inTable 5indicate that applying a framework with the presented features will enable preserving privacy when providing e-government services. In addition, the very positive feedback given by interviewees during the application of the PRE_EGOV in the EduPortal case study supported the usefulness of the proposed framework. The acceptance of the framework was evaluated by direct questions to stakeholders. Although, each stakeholder category confirmed that they accept the proposed framework approach, there were doubts between stakeholders whether the other party will accept the approach.

4) Generality of PRE_EGOV Framework

The successful application of the PRE_EGOV framework in the EduPortal case studyincreased confidence in the framework's applicability to other case studies. The PRE_EGOV framework development was informed by the defined RDs relevant to preserving privacy in e-government [1]. The main purpose of preserving privacy was defined based on an extensive literature review and consideration of existing privacy definitions in relevant frameworks. These RDs were discussed with experts in the area at relevant conferences and were validated using a general survey that included participants from different countries [1]. For these reasons, we argue that the proposed framework can be generalised and so could be applied to any e-government services in any country, but this would require long term evaluation and the application of the framework in many case studies in different countries.

5) Evaluation Limitations

The main limitation is that the PRE_EGOV framework was applied on only one case study. Although the application of the framework was successfuland the positive feedback was provided by relevant stakeholders supported the usefulness and acceptance of the framework, still the framework cannot be generalised based on one result without further investigation. However, this limitation can be treated by applying the framework in many case studies in different countries and evaluating the application of this framework in short and long term. Another limitation is that the researcher played the role of the facilitator who applied PRE_EGOV on the selected case study. This may have affected the successful application of the framework as the researcher is aware of all the steps and how they should be applied. However, this limitation can be treated in two ways. First, the PRE_EGOV framework should be used by other analysts in different case studies and feedback on obstacles faced when using the framework can be used to enhance the framework and to provide more details on how to apply different steps in the framework to enhance its generality. Also, details of successful application of the framework on different case studies should be well documented and made public where and when possible. These documented case studies can be used as a general guide on how the framework was applied in real world situations.With regard to EduPortal, the identified privacy requirements were considered in the updated version of the system and future study for user views regarding preserving privacy in the new system would be useful for a long-term evaluation

V. CONCLUSION

In this paper we discussed the application of the PRE_EGOV framework on a case study to demonstrate how the framework phases and elements can be applied. Applying the PRE_EGOV framework involved full engagement with relevant stakeholders at different phases of the application to identify the privacy requirements, verify and resolve any conflicts in the identified requirements and design the prototype. The identified privacy requirements were presented to stakeholders and agreed with them. The initial stakeholder's feedback about the framework was positive, however, a detailed evaluation through interviews was conducted following the application of the framework to evaluate the usefulness of the framework from different perspectives of the identified stakeholders.

Details of the evaluation interviews and discussion of the main findings were presented. Mainly the evaluation showed that PRE_EGOV framework is useable and accepted by stakeholders. The positive feedback on the application of the framework suggests that the framework is useful in preserving privacy in e-government. Finally, the application of the framework in the case study described in this paper presents the first round of action research and lessons learned from this application can be used for further enhancements to the framework. In addition, the framework cannot be generalised

unless it is applied in many case studies so refinements can be made according to the feedback gain after each application.

ACKNOWLEDGMENT

The researcher is deeply gratitude to the full collaboration of the officials in EduPortal with different roles who were so collaborative and thankfully considered the identified requirements in the new version of the systemwhich is used now by the time of this publication but due to confidentiality agreement names wont be mentioned.

REFERENCES

[1] Almagwashi, H. Preserving Privacy in E-government: A System Approach. in IFIP EGOV2012 and IFIP E-Part 2012 conference. Kristiansand, Norway 2012

[2] McCallister, E, Grance, T, and Scarfone, KA. Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),SP 800-122. NIST,Us Department of Commerce: US, 2010.

[3] OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD 2013. Available from: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[4] Privacy by Design. Information Commissioner's Office: UK, 2008.

[5] (2011) BSI. Privacy Framework, BSI,[Online]. Available from: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45123