Assessing Privacy Protection in Alumni Service

Kittisak Sa-Adaem and Yunyong Teng-Amnuay

***Abstract*—Most alumni do not realize their personal information should be protected. The problem is exacerbated by the lack in expertise on privacy issues and budget constraints in designing and enhancing privacy for alumni system. This research aims to provide an assessment guideline, called 7C, based on generic features, privacy patterns, privacy legal constraints, and privacy enhancing technologies (PETs), that will be helpful for software designer, developer, auditor, and end-user to deal with various aspects of privacy protections in their system. We selected Elgg, a popular open source social network software as the test system. We assessed Elgg using privacy detail specification (PDS) derived from our 7C methodology and recommended a list of plug-ins to augment its privacy protection.**

***Index Terms*—Alumni system, privacy guideline, privacy enhancing, elgg.**

I. Introduction

The information base grows rapidly under alumni activities. They share personal information, post comments, tag photos and so on. This comes under malicious or unintentional disclosure through powerful tools or search engines such as Google, Bing, and various intelligence applications that drill down into personal data. Alumni usually do not remember what personal information they gave to their alma mater while a student or engaged in alumni activities. Also, public institutions do not have adequate privacy expertises or funding to design and to continue enhancing their alumni system's privacy protection. This research surveyed and studied features of alumni and social system from various sources such as software shopping guide, alumni sites policy, OECD, privacy methodologies, technologies, privacy patterns, TRUSTe privacy requirements, and so on to create an alumni privacy analysis guideline for stronger privacy protection. We introduced a document called Privacy Detail Specification (PDS) and 7C Privacy Analysis Methodology consisting of Content, Confidential, Connectivity, Consent, Constraint, Control, and Construct. The 7C Privacy Analysis Methodology will be useful for developer, designer, auditor, and user to cope with privacy protection of their system.

II. Alumni Membership Service

An alumni site is a powerful online community for communication between alumni and their alma mater. This includes sharing personal activities, searching schoolmate, enrolling in an event, sharing knowledge, updating news, and so on. From CAPTERRA [1], a popular software shopping guide website, and existing detail design documents [2], [3], users of alumni site can be grouped as follows.

1) Anonymous users can search and view content that depends on consent of member and regulator constraint.
2) Alumni can login, deactivate, set privacy options, manage owner profile, data and relationship, do file sharing, post status, comment, register alumni event, access forum page, view another blog/profile, find alumni member, and use reporting service.
3) Group/Data administrator can manage event, group, use data sharing, set privacy options, and reporting.
4) System administrator can manage site content, account, role, group, sent mass mail, import/export data, and reporting.
5) Third-party user can access and use agreed upon information.

III. Data Privacy

A. Privacy Principle

Privacy allows an individual or group to reveal themselves selectively. Privacy uses the theory of natural rights, and generally responds to new information and communication technologies. In North America, Samuel D. Warren and Louis D. Brandeis wrote that privacy is the "right to be let alone" and focused on protecting individuals [4]. Kavakli et al. [5] summarized privacy requirement as

1) Anonymity: This is being virtually invisible or can be online without being tracked.
2) Pseudonymity: This is the ability to use a resource or service by acting under one or many pseudonyms, thus hiding real identity.
3) Unlinkability: This expresses the inability to link related information.
4) Unobservability: This protects users from being observed or tracked while browsing or using a service.

B. Privacy Constrain

In Thailand, the government passed laws for protecting personal information based on [6] the Organisation for Economic Co-operation and Development (OECD) [7]: guidelines. The guidelines cover personal information in the public and private sectors since 1980 [8] and represent an international consensus on how best to balance privacy protection with the free flow of personal data, are technology-neutral, flexible, allow for various means of compliance in all environments and have been put to use in

Manuscript received December 9, 2012; revised March 10, 2013.

Kittisak Sa-adaem is with Computer Science, Computer Engineering Department, Chulalongkorn University, Bangkok, Thailand (email: cpe_me@hotmail.com).

Yunyong Teng-amnuay is with Information Systems Engineering Laboratory, Computer Engineering Department, Chulalongkorn University, Bangkok, Thailand (e-mail: Yunyong.T@chula.ac.th).

various national regulatory and self-regulatory instruments. We also studied and included TRUSTe privacy requirement. TRUSTe is the leading online privacy solutions provider [9]. TRUSTe's privacy seal is recognized and trusted by millions of consumers.

IV. Related Work

A. Privacy Protection

The Privacy Enhancing Technologies (PETs) [10] is a generic term for a set of computer tools, applications and mechanisms which allow online services to protect the privacy of their customers' personally identifiable information (PII). PETs can be categorized as administrative tools, information tools, anonimizer tools, pseudonymizer tools, track and evident erasers and encryption tools. [11].

Kalloniatis et al. [11] introduced eight privacy process patterns namely identification, authentication, authorization, data protection, anonymity, pseudonymity, unlinkability, and unobservability.

Bouguettaya et al. [12] presented taxonomy of technology- and regulation-enabled solution for privacy preservation in the Web such as VPN, Firewall, PGP, Onion routing, etc.

Kavakli et al. [5] presented basic privacy requirement that should be considered during system design and development. They also introduced privacy implementation techniques that realize theses such as Anonimizer, Crowds, and Onion Routing.

B. Social Network Software

Deng et al. [13] presented misuse cases of social network 2.0 for privacy requirements and suggested mitigation strategies and techniques based LINDDUN privacy threat modeling methodology, and PETs.

Omar et al. [14] defined the primary and secondary social features and conducted an extensive evaluate for open source Web Content Management System (WCMSs) to facilitate Social Network Websites (SNWs). This incidentally Elgg was ranked as choice number 2 of open source WCMSs.

Curry et al. [15] presented an on-line collaborative data management system built on top of Elgg. They presented two reasons why Elgg is an ideal choice. Firstly, Elgg provides a powerful access control system that allows the owner to specify for any piece of content who can access and who can modify it. Secondly, the data in Elgg is extremely flexible, and allows arbitrary metadata to be applied to any object in the system. This is a strong baseline for building privacy-oriented alumni service.

V. Research Methodology

Our research methodology is depicted in Fig. 1. We analysed alumni website functionalities, then surveyed and gathered privacy requirements from multiple sources. Privacy knowledge are then gleaned from this analysis process. Analysis on privacy knowledge resulted in 7C Privacy Analysis Methodology, and Privacy Detail Specification (PDS). We created 7C Alumni Privacy Guideline based on 7C Privacy Analysis Methodology. We used the guideline to audit Elgg and suggested its existing plug-ins to support privacy protection. We leave those features unsupported by Elgg and its plug-ins for future consideration.

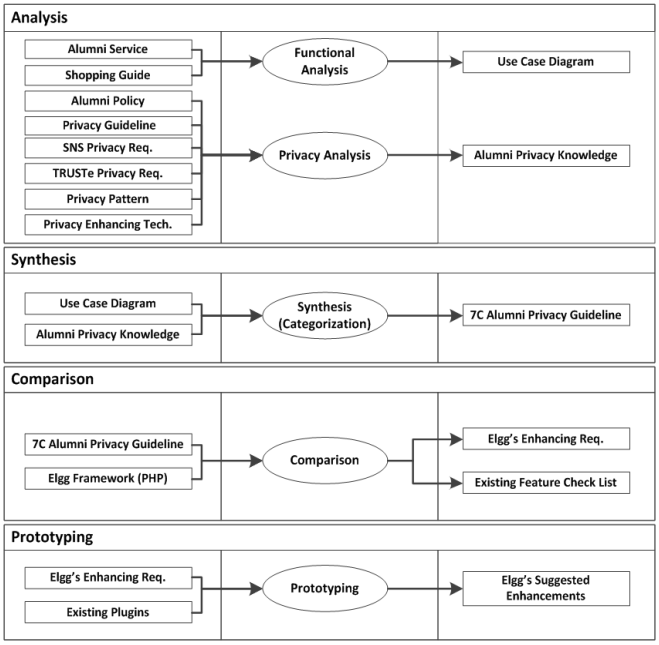

Fig. 1. Research methodology

VI. 7C Privacy Analysis Methodology

Analysis of privacy knowledge resulted in 7C Methodology. This makes it easier to grasp the complexity of the methodology. The "seven C's" are Content, Confidentiality, Connectivity, Consent, Constraint, Control, and Construct. Relationship of these 7 processes is depicted in Fig. 2 and each procedure is described below.

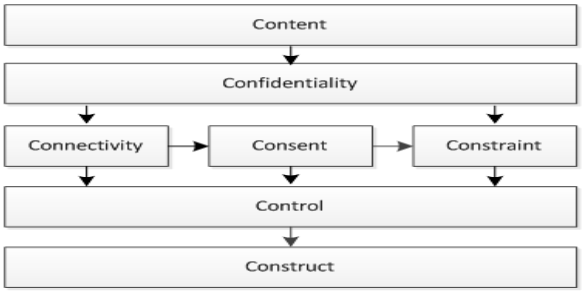

Fig. 2. Flow of 7C Privacy Analysis Methodology

A. Content

The first C is to gather and understand every piece of content in the system. In information architecture for the World Wide Web, Lou Rosenfeld and Peter Morville wrote, "We define content broadly as 'the stuff in your Web site.' This may include documents, data, applications, e-services, images, audio and video files, personal web pages, archived e-mail messages, and more [16]. All content are needed to be included. The list can be gathered from use-cases or software requirement specification. However, it is more convenient to extract content from screen shots and report forms as it is directly related to the use on "connectivity", described below. An example of content based on screen shot Elgg is depicted in Fig. 3.

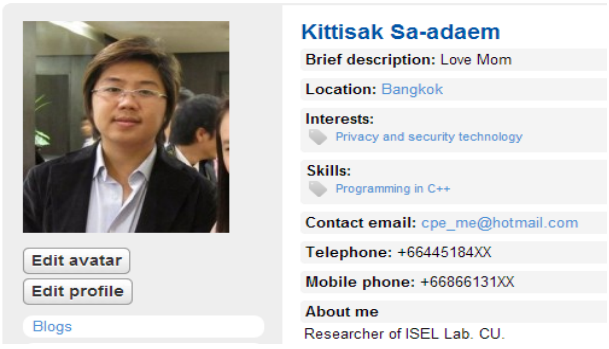

Fig. 3. Sample Elgg's personal profile.

B. Confidentiality

The second C is to specify which content consists of personal information that should be protected by system. To mark which attribute is personal information, US, UK, COPPA, EU, and other countries have defined list of personal data [17] and personal identifiable information (PII) [18], [19]. Following the definition of personal information, we can see that first name, last name, brief description, location, interests, skill, email, telephone, mobile phone number, and about me in Fig. 3 are personal information that should be marked as confidential. It is important to understand the difference between privacy and confidentiality [20] before starting this process:

1) Privacy is related to a person. For example a person may not want to be seen entering a place that might adversely affect their integrity, such as a pregnancy counselling centre.
2) Confidentiality refers to agreement about how a person's identifiable private information will be handled, managed, and disseminated.

C. Connectivity

The third C lists all connectivity and details each privilege between a function/service and personal information. Connectivity between a function/service and personal information that happen during use includes creating, reading, updating, and deleting. For example, as users update their locations or telephone numbers, anonymous search, or read alumni profile. Connectivity can be gathered from use cases, software requirement specification, and sequence diagrams.

D. Consent

The forth C lists all fields that the system allows alumni to control their disclosure for invoked connectivity such as mobile number, email, interests, and location. Essential fields, which are protected data, and theirs can be edited without verification can be credit card number, student ID, citizen ID, and so on. If the site does not support alumni consent functionality, alumni will react by not doing business with the site [21]. All consent required attributes depend on site policy and law.

Normal consent implies alumni consent on the private information already obtained from the customer and the service would like to give it (to third party). This implies the customer must implicitly, by default, give consent to the "primal" privacy information given to the service when accepting or applying for membership. In the concept of primal consent, customer must give consent to each piece of information required for membership registration and this will tie in with the level of service the customer will receive.

At present, all services have a very coarse grain consent, i.e., if the customer needs the service then the customer have to give consent to a lump-sum package of personnel information to obtain a package of services. A more fine-grained service and consent pairing should be developed. A customer may withhold his birthday and will not receive gift voucher on his birthday. If he deems the voucher valuable enough he will give consent for the service to obtain his birthday by providing the information himself. This kind of consent granularity can evolve into a trust relationship between the customer and the service.

E. Constraint

The fifth C is to survey and list all rules, regulators, and guidelines. Usually constraint depends on country and service provider. All constraints will help site to enable privacy protection and to protect itself not to violate privacy law.

F. Control

The sixth C is to specify privacy control for each constraint. At the start of this research, we surveyed privacy enhancing frameworks and guidelines. We found LINDDUN framework to applicable [13]. Kumari's requirement analysis for privacy in social networks [22] and Intel's privacy requirements and recommendations [23] are also useful to follow and apply. To fulfill LINDDUN's web 2.0 suggested mitigation strategies and techniques, we merged Intel's privacy requirements and recommendations into entity/user (U), data store (DS), data flow (DF), and process (P) as targets for controls. We also matched privacy process patterns [11] with LINDDUN's threat categories to support designer working on software design phase as depicted in Table I. The result of merging LINDDUN's, Kumari's, and Intel's is shown in table name "Control" , a member of privacy detail specification in Fig. 5.

TABLE I: MAPPING LINDDUN THREAT CATEGORY WITH PRIVACY PROCESS PATTERN AND GUIDELINE

LINDDUN's threat category	Privacy Properties	E	DF	DS	P	Pattern/ Guideline
Linkability	Unlinkability	x	x	x	x	Unlinkability
Identifiability	Anonymity and Pseudonymity	x	x	x	x	Anonymity Pseudonymity
Non-repudiation	Plauusible deniability		x	x	x	
Detectability	Undetectability and Unobservability		x	x	x	Unobservability
Information **D**isclosure	Confidentiality		x	x	x	Authentication Authorization Identification Data Protection
Content **U**nawareness	Content awareness	x				OECD & TRUSTe
Policy/Consent **N**oncompliance	Policy and Consent compliance	x	x	x	x	OECD & TRUSTe

G. Construct

The seventh C is to select PETs [10], security technology, some software finesses technique to affect privacy control,

and anonymity related implementation such as k-anonymity [13], Tor [24], and so on. Designer can select PETs by matching with privacy process pattern in Figure 4. Moreover, Deng et al. [13] also provided table of mapping privacy objectives with PETs. Selecting suitable PETs depends on budget, system architecture, scalability, level of privacy protection, time to market, and so on. The security safeguard is very important to ensure privacy protection, and because it is the first time of defense to prevent and protect intruder from accessing personal information. Many security recommendations are suggested in [12], [24]-[26] such as firewall, SSL, HTTPS, and so on.

	Administrative Tools					Information Tools			Anonymizer Products, Services and Architectures										Pseudonymizer Tools		Track and Evident Erasers				Encryption Tools		
	Identity Management	Biometrics	Smart Cards	Permission Management	Monitoring and Audit tools	Privacy Policy Generators	Privacy Policy Readers	Privacy Compliance Scanning	Browsing Pseudonyms	Virtual Email Addresses	Trusted Third Parties	Surrogate Keys	Crowds	Onion Routing	DC-Nets	Mix-Nets	Hordes	GAP	Tor	CRM Personalization	Application Data Management	Spyware Detection and Removal	Browser Cleaning Tools	Activity Traces eraser	Harddisk data eraser	Encrypting Email	Encrypting Transactions	Encrypting Documents
Authentication	X	X	X	X	X																							
Authorization	X	X	X	X	X																							
Identification	X	X	X	X	X																							
Data Protection	X	X	X	X	X	X	X	X																				X
Anonymity and/or pseudonymity	X	X	X	X					X	X	X		X	X	X	X	X	X	X	X	X				X			
Unlinkability											X	X		X		X	X	X	X	X	X		X	X	X			
Unobservability			X	X	X												X	X	X		X		X	X	X	X	X	X

Fig. 4. Mapping between privacy process patterns and PETs.

VII. Result

A. A Sample Privacy Detail Specification of Alumni Service

When applying the 7C to an alumni service we obtain its Privacy Detail Specification, or PDS. A sample of the PDS is depicted in Fig. 5.

B. Assessing Elgg

We studied handbook of Elgg version 1.8 [26], reviewed Elgg's plug-ins [27], related researches [14], [15] and online recommends [28]-[30]. We found Elgg has 1653 plug-ins and 39 of these are apparently privacy enhancing related. List of Elgg's core functionalities and plug-ins to support privacy protection is presented in Table II.

We assessed Elgg version 1.8 based on our recommended 23 privacy related features as summarized from PDS in Fig. 5. There are 4 features not supported by Elgg and its existing plug-ins, and 9 privacy related plug-ins support only the previous Elgg version 1.7. The four missing features are primal consent, disabling search engine, unlinkability, and unobservability. These are feature that should be present in alumni or similar social network system. For example, Facebook service allows users to prevent search engines like Google to access their data ("who can look me up" [31]).

C. Primal Consent on Privacy Policy

Table III shows the page count of privacy agreement by well-known sites. These agreements are written in obscure and difficult-to-understand lawyer language. A privacy agreement usually aims at course grained consent by the customer. There are even controversies on this issue [32].

TABLE III: Total number of Pages of Popular Site's Policy

Site	AT&T	Myspace	Skype	WhatApp	Facebook	Ebay	Google+	Linked-in	Amazon	IBM	Apple	LINE	Twitter
Total	23	17	12	11	7	7	7	7	6	6	4	4	4

TABLE II: Assessing Elgg

Recommended Privacy related features	Elgg 1.8 Core	Elgg 1.7 Plug-ins	Elgg 1.8 Plug-ins
Choice on agreement			Registration Term 1.2.1
Mandatory fields control			Profile Manager 7.5
Primal consent			
Registration validation	x	Site Access 2.6	User validation by admin 1.0
Privacy by default	x		
Data retention period			Expirationdate 1.8.1
Fine-grain access control	x		SW Social Privacy Concord
Role base access control		Group access 1.2.2	Access Collection Management 1.0.0, Roles for Elgg 1.0.0, Group Administrators 1.0.0
Individual access	x		
Easy privacy setting	x		
Disclosure over consent	x		
Transferring after consent			Social Share Privacy 1.8-12.01.22
Authentication and identity	x	Linkedin service 1.0, Login by Email 0.2, CAS Auth 0.2, OpenID client 1.3	Persona 1.0, SAML authentication 1.3, Simple Google Authentication 1.1, LDAP authentication 0.2, Facebook Connect Login 1.1
Disable search engine			
Blocking and backlist	x		Lee's block user 1.0.4, Spam Throttle 1.5
Privacy leak monitoring	x		Who viewed me 1.1, Advance Statistics 0.1
User feedback channel		Help Chat/Live Support & Site Feedback 0.1	Questions and Answers 1.0, Brainstorm your Elgg 0.4
User deactivate cleaner	x	Westor deleteMe 1.1	Site Cron 1.8.9, Comasis Cancel Account 1.8, Member Selfdelete 1.0
Anonymity	x		Disqus Elgg 2
Pseudonimity	x		Tabbed Profile 1.7
Unlinkabiblity			
Unobservability			
Security safeguards	x	Password expiration 1.1	Spam checker 1.8.2, Upgrade Key 1.0, Image CAPTCHA 2.0, Spam Login Filter 1.8.2, Elgg-crypt 1.8.0

Content:

ID	Name (Content of view)	User	Purpose of used
1	My profile	Alumni	Setup owner profile
2	Another profile	Alumni	View other alumni profile
3	List of alumni	Anonymous	View list of alumni
4	Member profile	Data Admin	Update alumni profile
5	List of donation	3-Party	Extract allowed data

Confidentiality: e=Existing, and Cte#=Content's ID.

ID	Name	Cte#1	Cte#2	Cte#3	Cte#4	Cte#5
1	Student ID	e			e	
2	Name	e	e	e	e	e
3	Birthday	e	e		e	
4	Class	e	e	e	e	
5	Grade	e			e	
6	Donation amount	e			e	e
7	Favorite quotations	e	e			
8	Address	e			e	
9	Current salary					
10	Religion					

Connectivity: a=Allow.

ID	Content's Name	Confidentiality's Name	C	R	U	D
1	My profile	Student ID		a		
2	My profile	Name		a		
3	My profile	Birthday		a		
4	My profile	Class		a		
5	My profile	Grade		a		
6	My profile	Donation amount		a		
7	My profile	Favorite quotations	a	a	a	a
8	My profile	Address	a	a	a	
9	Another profile	Name		a		
10	Another profile	Class		a		
11	Another profile	Birthday		a		
12	Another profile	Favorite quotations		a		
13	List of alumni	Name		a		
14	List of alumni	Class		a		
15	Member profile	Student ID	a	a	a	
16	Member profile	Name	a	a	a	
17	Member profile	Birthday	a			a
18	Member profile	Class	a	a	a	
19	Member profile	Grade	a		a	
21	Member profile	Donation amount	a		a	
22	Member profile	Address		a	a	
23	List of donation	Name		a		
24	List of donation	Donation amount		a		

Consent: t=Toggle.

ID	Connectivity's ID	Confidentiality's Name	C	R	U	D
1	11	Birthday		t		
2	12	Favorite Quotations		t		
3	13	Name		t		
4	14	Class		t		
5	22	Address			t	
6	23	Name		t		
7	24	Mobile number		t		

Constraint:

ID	Name	Source	Constraint Detail
1	Collection Limit	OECD [7]	There should be limits to the collection of personal data and any such data should be obtained by lawful …
2	Data Quality	OECD	Personal data should be accurate, complete and kept up-to-date…
3	Purpose Specification	OECD	The purposes for which personal data are collected should be specified….
4	Use Limitation	OECD	Personal data should not be disclosed, made available or otherwise used for purposes…
5	Security Safeguards	OECD	Personal data should be protected by reasonable security safeguards against…
6	Openness	OECD	There should be a general policy of openness about developments … with respect to personal data …
7	Individual Participation	OECD	An individual should have the right a) to obtain from a data controller, or otherwise …
8	Accountability	OECD	A data controller should be accountable for complying with measures …
9	Consent and Choice	Bevanda et al. [33]	The purpose associated with personal information shall have consent of the donor of personal information
10	Data Retention	TRUSTe [9]	The time period of retention PII, How log system will retain that information.
11	Third Party and Transborder	Skinner et al. [34]	The information system may not transfer information to a third party or foreign country without the consent of the individual
12	Search Service	TRUSTe	The system shall provide the individual a mechanism to stop having their information displayed in search result.
13	Anonymity	Skinner et al.	The information system should be done in way that supports anonymity for the individual user.
14	Pseudonymity	Kavakli et al. [5]	System should provide ability to use a resource or service by acting under one or many pseudonyms, thus hiding real identity.
15	Unlinkability	Kavakli et al.	System should provide inability to link related personal information.
16	Unobservability	Kavakli et al.	System should protect users from being observed while browsing or using a service.

Control:

ID	Type	How to control software design and development.
1	Collection Limit	**Data Store**) Do not retain information longer than necessary. Do not collect individual's personal information if not needed. **User**) Use feedback tools to raise user's privacy awareness.
2	Data Quality	**Process**) All personal information about an individual must be available to that individual and allow them to make corrections and update.
3	Purpose Specification	**User**) 1. The user must be informed about what is being collected, and why and whether the information will be shared with anyone else. 2. Provide brief description of your privacy policy with a link to more detailed version.
4	Use Limitation	**Process**) 1. Personal information may only be used for the purpose described in the notice. 2. Apply access control according to user's privacy preference
5	Security Safeguards	**Data Store**) Protected by reasonable security safeguards. **Data Flow**) When collecting personal information online, implement encryption techniques, and employ secure communication. **Process**) 1. Use principle of least privilege. 2. Avoid display object references whenever possible. 3. Confirm that user has the necessary privileges and authorization. 4. Avoid the use of custom cookies. 5. Validate input to a guard against Cross-Site Scripting. 6. Completing a code review.
6	Openness	**User**) The information system must have documented and make easily available its policies on personal information.
7	Individual Participation	**Process**) 1. Allow the individual to maintain his own personal information. 2. Use a secure user profile.
8	Accountability	1. Appoint employee responsible for policy compliance or hire external company for compliancy auditing. 2. Ensure training obligation for employees.
9	Consent and Choice	**Process**) 1. Obtain affirmative opt-in consent from an individual before collecting their personal information. 2. Inform the individual of their choices and require the individual to select before proceeding. **User**) Add a convenient location in the source for personal information handling practices.
10	Data Retention	**Data Store**) All personal information should have expiration date. **User**) Inform how long you will retain the personal information.
11	Third party and Transborder	**Process**) Obtain the user's permission before sharing collected personal information with third parties. **User**) When transferring the personal information to third parties, you need to inform the individual. You need to honor their decision
12	Search Service	**Process**) Provide mechanism to stop having their information displayed in search result. **User**) Privacy statement shall state how individual can remove their information from displayed search result.
13	Anonymity	**Data Store**) Apply data anonymization techniques, and enforce data protection by means of relationship-based access control. **Data Flow**) Deploy anonymity system for communication between user and site. **Process**) Use identity management to ensure unlinkability.
14	Pseudonymize	**Process**) Apply secure pseudonumization techniques to issue pseudonyms as user IDs. **User**) Use privacy awareness: Inform users using real ID runs a risk for privacy violation.
15	Unlinkability	**Data Store**) Apply data anonymization techniques. **Data Flow**) Deploy anonymity system. **Process**) Deploy anonymity system to support unlinkability of pseudonyms. **User**) Use privacy awareness: Inform users that revealing too much information online can be privacy invasive.
16	Unobservability	**Data Store**) Use sufficient access control and information hiding techniques. **Data Flow**) Covert channel and steganography can be used to protect privacy.

Construct:

ID	Name	Short Detail	Control Type
1	K-anonymity	Each individual's record is indistinguishable from at least k-1 other's records.	Anonymization technique
2	Pseudonymization	Render the data record less identifying.	Pseudonymization technique
3	Feedback	To raise user's privacy awareness.	Privacy Awareness
4	Primal consent	To explicitly allow individual of their choices in providing privacy information using options, radio buttons, etc.	Consent & Choice
5	Site's Policy	A statement or a legal document.	Privacy Awareness
6	OpenID	Allows users to be authenticated by certain co-operating sites.	Authentication & Identity
7	XACML	Access control policy language implemented in XML	Access Control
8	LDAP	Lightweight Directory Access Protocol.	Access Control
9	Tor	The Onion Router is a system intended for online anonymity.	Anonymity System
12	HTTPS	Hypertext Transfer Protocol Secure.	Security Safeguards
13	SNORT	Network intrusion prevention system.	Security Safeguards
14	Firewall	Prevent unauthorized communications between computer networks or hosts.	Security Safeguards
15	P3P	A protocol allowing websites to declare their intended use of information they collect about web browser users.	Security Safeguards

Fig. 5. A sample Privacy Detail Specification of Alumni Service

VIII. Conclusion and Future Work

Privacy protection is related to many constituent parts such as consents, laws, control methodologies, security technologies, and so on. This is not easy for a person who is not a privacy expert. To make privacy enhancing process

easier, we introduced 7C. This will be helpful for stakeholders to deal with various aspects of privacy protections in their system. Applying the methodology to alumni service will result in Privacy Detail Specification which aids in privacy protection of the service.

Elgg is a popular open-source social network software and has good roadmap. It is suitable for use as our prototype alumni system for assessment on privacy. To fulfill privacy protection, developer and designer select suitable existing plug-ins and build new plug-ins for missing controls. Thus our work extends from simply assessment to a more practical guideline as compared to previous work [35].

Our research also indicates that the primal consent is important and should not be ignored. Currently systems collect their member personal information in term of package with very coarse granularity. The granularity of consent over personal information is neglected during use by system, transfer to third party, or when member exchange their personal information with site to receive some services. Our future work is the development of Elgg's plug-ins to support privacy protection based on concept of primal consent and privacy requirements that Elgg does not support via current core functionality and existing plug-ins.

REFERENCES

[1] CAPTERRA. Alumni Management Software Programs. [Online]. Available: http://www.capterra.com/alumni-management-software

[2] L. Jarupakwittaya and H. Naknarong, "Alumni Management System," Senior Project, Dept. CS, Khon Kaen Univ., Thailand, 2009.

[3] T. Jaiswal and R. Zhu, "Software Requirements Specification for Larkut.com," Herguan Univ., Sunnyvale, CA, 2010.

[4] Wikipedia. Privacy. [Online]. Available: http://en.wikipedia.org/wiki/Privacy.

[5] E. Kavakli, C. Kalloniatis, and S. Gritzalis , "Addressing privacy: matching user requirements to implementation techniques," in *Proc. the 7th Hellenic European Research on Computer Mathematics & its Applications Conf.*, Athens, Greece, September 22 - 24, 2005.

[6] RTGS. Notification on the Electronic Transactions Commission on Policy and practice Statement on Personal Data Protection of a Government Agency 2010. [Online]. Available: http://www.ratchakitcha.soc.go.th/DATA/PDF/2553/E/126/31.PDF

[7] OECD. About the OECD. [Online]. Available: http://www.oecd.org/about/.

[8] OECD. Privacy and Personal Data Protection. [Online]. Available: http://www.oecd.org/sti/interneteconomy/37626097.pdf.

[9] TRUSTe. Privacy Program Requirements. [Online]. Available: http://www.truste.com/privacy-program-requirements.

[10] Wikipedia. Privacy-enhancing technologies. [Online]. Available: http://en.wikipedia.org/wiki/Privacy-enhancing_technologies.

[11] C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Using Privacy Process Patterns for Incorporating Privacy Requirements into the System Design Process," in *Proc. the 2sd International Conf. on Availability, Reliability and Security*, pp. 1009-1017, April 10-13 2007

[12] A. R. A. Bouguettaya and M. Y. Eltoweissy, "Privacy on the Web: facts, challenges, and solutions," *IEEE Security & Privacy*, vol. 1, no. 6, pp. 40- 49, Nov.-Dec. 2003.

[13] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements," *Requirements Engineering*, vol. 16, no. 1, pp 3-32, 2011.

[14] O. Al-hamdi and A. Salah, "Open Source Web Content Management Systems to Build Social Network Websites," *International Journal of Reviews in Computing*, vol. 11, pp. 48-60, Sep. 30, 2012.

[15] R. Curry, C. Kiddle, R. Simmonds, and G. Z. Pastorello, "An on-line collaborative data management system," *Gateway Computing Environments Workshop*, pp. 1-10, Nov. 14, 2010.

[16] Wikipedia. Web content. [Online]. Available: http://en.wikipedia.org/wiki/Web_content

[17] The IT Law Wiki. Personal Data. [Online]. Available: http://itlaw.wikia.com/wiki/Personal_data.

[18] The IT Law Wiki. Personally identifiable information. [Online]. Available: http://itlaw.wikia.com/wiki/Personally_identifiable_information

[19] Wikipedia. Personally identifiable information. [Online]. Available: http://en.wikipedia.org/wiki/Personal_information

[20] UT Health Science Center. Do you know the difference between Privacy and Confidential?. [Online]. Available: http://research.uthscsa.edu/ocr/Privacy%20and%20Confidentiality%20in%20Human%20Research.pdf

[21] L. L. Lobato, E. B. Fernandez, and S. D. Zorzo, "Patterns to Support the Development of Privacy Policies," in *Proc. International Conf. on Availability, Reliability and Security*, pp. 744-749, March 16-19, 2009.

[22] P. Kumari, "Requirements analysis for privacy in social networks," in *Proc. 8th International Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods*, Namur, October 2010.

[23] Privacy Requirements and Recommendations for Application Development for the Intel AppUp developer program: What Application Developers Should Know. [Online]. Available: http://software.intel.com/en-us/articles/privacy-requirements-and-recommendations-for-application-development-for-the-intel-appupsm.

[24] S. Romanosky, A. Acquisti, J. Hong, L. F. Cranor, and B. Friedman, "Privacy patterns for online interactions," in *Proc. of the conf. on Pattern languages of programs*, ACM, NY, USA, Article 12, 2006.

[25] A. G. Abbasi, S. Muftic, and I. Hotamov, "Web Contents Protection, Secure Execution and Authorized Distribution," *5th International Multi-Conf. on Computing in the Global Information Technology*, pp. 157-162, Sep. 20-25, 2010.

[26] C. Costello, *Elgg 1.8 Social Networking*, 2sd ed., Birmingham, B3, 2PB, UK, Feb, 2012.

[27] Elgg. Welcome to Elgg's plugin directory. [Online]. Available: http://community.elgg.org/plugins

[28] Wikipedia. Comparison of social networking software. [Online]. Available: http://en.wikipedia.org/wiki/Comparison_of_social_networking_software

[29] D. Fory. Social Network / Community / Forum Software Comparison Chart. [Online]. Available: http://www.deanflory.com/articles/social_software_comparison

[30] M. Sharma. Users, Profiles, and Connections in Elgg. (April, 2008). [Online]. Available: http://www.packtpub.com/article/users-profiles-and-connections-in-elgg

[31] Facebook. Making Your Settings Easier to Find: Dig Into the Details. [Online]. Available: https://www.facebook.com/about/details.

[32] AppleInsider. US congressmen inquire about iOS privacy with Apple, 33 developers. [Online]. Available: http://appleinsider.com/articles/12/03/22/us_congressmen_inquire_about_ios_privacy_with_apple_33_developers

[33] V. Bevanda, J. Azemovic, and D. Music, "Privacy Preserving in eLearning Environment (Case of Modeling Hippocratic Database Structure)," presented at 4th Balkan Conf. in Informatics, pp. 47-52, Sep.17-19, 2009.

[34] G. Skinner, S. Han, and E. Chang, "A framework of privacy shield in organizational information systems," *International Conf. on Mobile Business*, pp. 647- 650, July 11-13, 2005.

[35] D. W. Yu, S. Doddapaneni, and S. Murthy, "A Privacy Assessment Approach for Serviced Oriented Architecture Application," *2sd IEEE International Workshop in Service-Oriented System Engineering*, pp. 67-75, Oct. 2006

Kittisak Sa-Adaem was born in Surin, Thailand in 1982. He graduated from Kasetsart University with Bachelor Degree in Computer Engineering. He is currently a master student in Computer Science, a member of Information Systems Engineering Laboratory in the Department of Computer Engineering, Chulalongkorn University, and a senior SM in Telecom Billing System of Amdocs (Thailand) Co., Ltd.

Yunyong Teng-Amnuay was born in Bangkok, Thailand in 1954. He graduated from Chulalongkorn University with Bachelor Degree in Electrical Engineering and Master Degree in Computer Science. He obtained Ph.D. in Computer Science from Iowa State University, U.S.A, in 1984. His expertises are in system software, distributed systems, networking, and information system architecture. He is currently a lecturer and the director of Information Systems Engineering Laboratory of the Department of Computer Engineering, Chulalongkorn University.