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

DOI: 10.7763/IJCEE.2013.V5.745 424
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, anonymizer tools, pseudonymizer tools, track and evident erasers and encryption tools. [11].


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 these 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.

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.

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.
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>
<thead>
<tr>
<th>LINDDUN’s Threat Category</th>
<th>Pattern and Guideline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linkability</td>
<td>Unlinkability</td>
</tr>
<tr>
<td>Identification</td>
<td>Anonymity and Pseudonymity</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>Plausible deniability</td>
</tr>
<tr>
<td>Detectability</td>
<td>Undetectability and Unobservability</td>
</tr>
<tr>
<td>Information Disclosure</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>Content Unawareness</td>
<td>x</td>
</tr>
<tr>
<td>Policy/Consent Noncompliance</td>
<td>Policy and Consent compliance</td>
</tr>
<tr>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

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.

![Fig. 4. Mapping between privacy process patterns and PETs.](image)

**TABLE II: ASSESSING ELLGG**

<table>
<thead>
<tr>
<th>Recommended Privacy related features</th>
<th>Elgg 1.8 Core</th>
<th>Elgg 1.7 Plug-ins</th>
<th>Elgg 1.8 Plug-ins</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choice on agreement</td>
<td>Registration Term 1.2.1</td>
<td>Profile Manager 7.5</td>
<td></td>
</tr>
<tr>
<td>Mandatory fields control</td>
<td>x</td>
<td>User validation by admin 1.0</td>
<td></td>
</tr>
<tr>
<td>Primal consent</td>
<td>x</td>
<td>Site Access 2.6</td>
<td></td>
</tr>
<tr>
<td>Registration validation</td>
<td>x</td>
<td>SW Social Privacy Conceal</td>
<td></td>
</tr>
<tr>
<td>Privacy by default</td>
<td>x</td>
<td>Group access 1.2.2</td>
<td></td>
</tr>
<tr>
<td>Data retention period</td>
<td>x</td>
<td>Access Collection Management 1.0.0, Roles for Elgg 1.0.0, Group Administrators 1.0.0</td>
<td></td>
</tr>
<tr>
<td>Fine-grain access control</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Role base access control</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Individual access</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Easy privacy setting</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Disclosure over consent</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Transferring alter consent</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Authentication and identity</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Authentication and identity</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Blocking and backlist</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Privacy leak monitoring</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>User feedback channel</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>User deactivate cleaner</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Security safeguards</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Anonymity</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Pseudonymity</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Unlinkability</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Unobservability</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Password expiration</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

**TABLE III: TOTAL NUMBER OF PAGES OF POPULAR SITE’S POLICY**

<table>
<thead>
<tr>
<th>Site</th>
<th>AT&amp;T</th>
<th>MySpace</th>
<th>Skype</th>
<th>Yahoo</th>
<th>Facebook</th>
<th>Elgg</th>
<th>Google+</th>
<th>LinkedIn</th>
<th>Amazon</th>
<th>IBM</th>
<th>Apple</th>
<th>LINE</th>
<th>Tweet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>23</td>
<td>17</td>
<td>12</td>
<td>11</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>6</td>
<td>6</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>
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
Our research also indicates that the primal consent is important and should not be ignored. Currently systems collect their 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 Eigg’s plug-ins to support privacy protection based on concept of primal consent and privacy requirements that Eigg does not support via current functionality and existing plug-ins.

REFERENCES


Kittisaik 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-Amnay 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 expertise 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.