แนวทางเกี่ยวกับความเป็นส่วนตัวสำหรับระบบบริการข้อมูลสมาชิกศิษย์เก่าโดยอาศัยแบบรูปความเป็นส่วนตัว

นายกิตติศักดิ์ สะอาดเอี่ยม

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2555

PRIVACY GUIDELINE FOR ALUMNI MEMBERSHIP SERVICE BASED ON PRIVACY PATTERN

Mr. Kittisak Sa-adaem

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science Program in Computer Science

Department of Computer Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2012

หัวข้อวิทยานิพนธ์	แนวทางเกี่ยวกับความเป็นส่วนตัวสำหรับระบบบริการข้อมูลสมาชิกศิษย์เก่าโดยอาศัยแบบรูปความเป็นส่วนตัว
โดย	นายกิตติศักดิ์ สะอาดเอี่ยม
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	อาจารย์ ดร.ยรรยง เต็งอำนวย

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

…….. คณบดีคณะวิศวกรรมศาสตร์
(รองศาสตราจารย์ ดร.บุญสม เลิศหิรัญวงศ์)

คณะกรรมการสอบวิทยานิพนธ์

……. ประธานกรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.เกริก ภิรมย์โสภา)

…….. อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(อาจารย์ ดร.ยรรยง เต็งอำนวย)

……. กรรมการภายนอกมหาวิทยาลัย
(ผู้ช่วยศาสตราจารย์ ดร.ชวลิต ศรีสถาพรพัฒน์)

กิตติศักดิ์ สะอาดเอี่ยม : แนวทางเกี่ยวกับความเป็นส่วนตัวสำหรับระบบบริการข้อมูลสมาชิกศิษย์เก่าโดยอาศัยแบบรูปความเป็นส่วนตัว. (Privacy Guideline for Alumni Membership Service based on Privacy Pattern) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: อาจารย์.ดร.ยรรยง เต็งอำนวย, 50 หน้า.

สมาชิกระบบบริการข้อมูลสมาชิกศิษย์เก่าส่วนใหญ่ไม่ได้ตระหนักว่าข้อมูลส่วนบุคคลของตัวเองควรได้รับการปกป้อง อีกทั้งปัญหาด้านการปกป้องข้อมูลส่วนบุคคลยังถูกยกระดับให้มีความรุนแรงมากขึ้นเพราะขาดผู้เชี่ยวชาญทางด้านการรักษาความเป็นส่วนตัว และเนื่องด้วยข้อจำกัดในเรื่องงบประมาณที่จะนำมาใช้ในการพัฒนาและปรับปรุงการรักษาความเป็นส่วนตัวของระบบบริการข้อมูลสมาชิกศิษย์เก่าให้ดีขึ้น งานวิจัยนี้มีเป้าหมายเพื่อพัฒนาแนวทางในการรักษาความเป็นส่วนตัว โดยนำเสนอแนวทางและขั้นตอนวิธีในการที่จะทำให้ระบบบริการข้อมูลสมาชิกศิษย์เก่าสามารถรักษาความเป็นส่วนตัวได้ดีมากขึ้น เรียกวิธีการนี้ว่า เซเว่นซี (7C) โดยมีพื้นฐานบนการทำงานทั่วไปของระบบข้อมูลสมาชิกศิษย์เก่า แบบรูปความเป็นส่วนตัว ข้อบังคับในการรักษาความเป็นส่วนตัว และเทคโนโลยีที่จะนำมาช่วยในการรักษาความเป็นส่วนตัว เพื่อช่วยให้ผู้ออกแบบระบบ ผู้พัฒนาระบบ ผู้ตรวจสอบระบบ และตัวผู้ใช้งานระบบเอง สามารถเข้าใจและจัดการเรื่องความเป็นส่วนตัวได้ งานวิจัยนี้ได้เลือกซอฟต์แวร์อีแอลจีจี (Elgg) ที่ได้รับความนิยมสูงสำหรับการพัฒนาระบบเครือข่ายสังคมออนไลน์เป็นกรณีศึกษา พร้อมทั้งได้ทำการประเมินระบบอีแอลจีจี ด้วยเอกสาร Privacy Detail Specification ซึ่งเป็นเอกสารที่ได้จากขั้นตอนต่างๆ ทั้งเจ็ดตามขั้นตอนวิธีการเซเว่นซี และยังได้นำเสนอรายการของปลั๊กอินที่เกี่ยวข้องกับการรักษาความเป็นส่วนตัวสำหรับระบบอีแอลจีจีด้วย

ภาควิชา วิศวกรรมคอมพิวเตอร์ ..... ลายมือชื่อนิสิต .....

สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์ ..... ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก .....

ปีการศึกษา 2555 .....

5271407021 : MAJOR COMPUTER SCIENCE
KEYWORDS : ALUMNI SYSTEM / PRIVACY GUIDELINE / PRIVACY ENHANCING / ELGG

KITTISAK SA-ADAEM : PRIVACY GUIDELINE FOR ALUMNI MEMBERSHIP SERVICE BASED ON PRIVACY PATTERN. ADVISOR : YUNYONG TENG-AMNUAY,Ph.D., 50 pp.

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 derived from our 7C methodology and recommended a list of plug-ins to augment its privacy protection.

Department : Computer Engineering Student's Signature .....
Field of Study : Computer Science Advisor's Signature .....
Academic Year : 2012 .....

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปด้วยดีด้วยความกรุณาช่วยเหลือจาก อาจารย์ ดร.ยรรยง เต็งอำนวย ซึ่งเป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ ท่านได้กรุณามอบความรู้ คำแนะนำ ตรวจทานเพื่อแก้ไขส่วนบกพร่องของงานวิจัย ตลอดจนการตรวจทานแก้ไขวิทยานิพนธ์ให้มีความสมบูรณ์ นอกจากนี้ผู้เขียนยังได้รับความกรุณาจาก ผศ.ดร.เกริก ภิรมย์โสภา ประธานกรรมการสอบวิทยานิพนธ์ รวมถึง ผศ.ดร.ชวลิต ศรีสถาพรพัฒน์ กรรมการสอบวิทยานิพนธ์ผู้ทรงคุณวุฒิจากภายนอก ที่ได้ให้คำแนะนำ รวมทั้งข้อเสนอแนะต่างๆ ที่เป็นประโยชน์เพื่อนำมาใช้ปรับปรุงวิทยานิพนธ์ให้เกิดความสมบูรณ์มากยิ่งขึ้น

ผู้เขียนขอกราบขอบพระคุณบิดา มารดา และคุณป้าของข้าพเจ้าที่คอยเป็นกำลังใจให้เสมอมา รวมทั้งเพื่อนสนิทของข้าพเจ้า คุณธนชนม์ ชีพบริสุทธิกุล และ คุณอรรถพล พวงพุ่ม ที่ได้ฝ่าฟันศึกษาและทำงานวิจัยมาด้วยกัน เป็นทั้งเพื่อนและที่ปรึกษา คอยให้กำลังใจกันและกัน คุณประภาวดี เอกวงศ์ ที่คอยช่วยเหลือเรื่องการเดินเอกสารต่างๆ ขอขอบคุณ เพื่อนๆ พี่ๆ และอาจารย์ทุกท่านที่ข้าพเจ้าไม่ได้เอ่ยนาม ซึ่งเคยช่วยเหลือข้าพเจ้า ถ่ายทอดความรู้ให้ข้าพเจ้า และเป็นแรงบันดาลใจให้ข้าพเจ้าเสมอมา

สารบัญ

หน้า

หน้า

สารบัญตาราง

หน้า

สารบัญภาพ

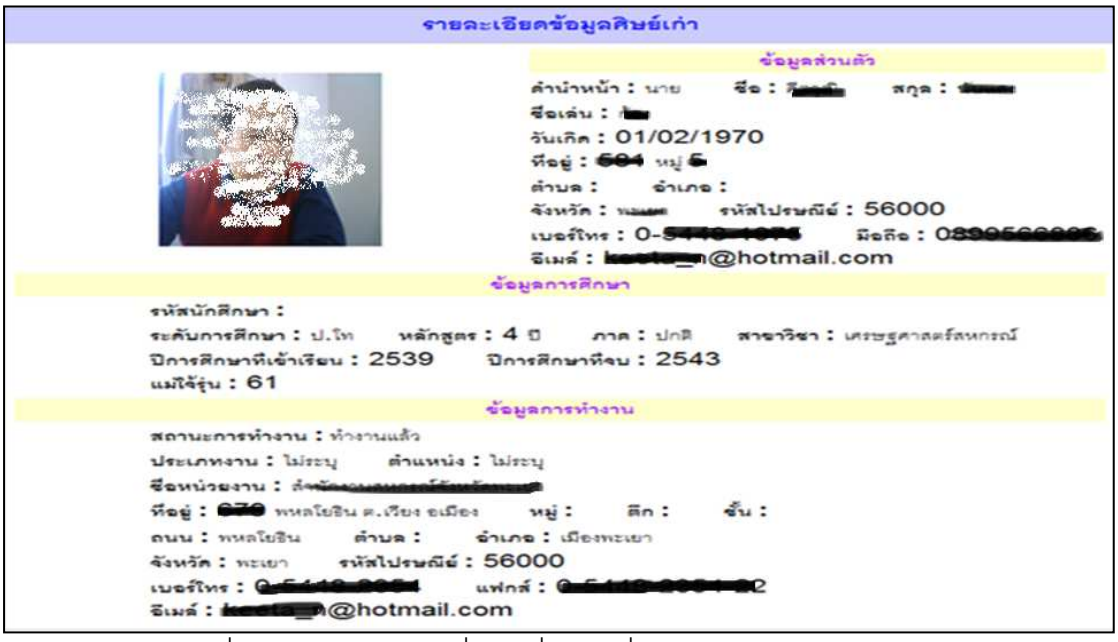
หน้า

บทที่ 1

บทนำ

1.1. ความเป็นมาและความสำคัญของปัญหา

เนื่องจากการพัฒนาและการเลือกใช้ซอฟต์แวร์ระบบบริการข้อมูลสมาชิกศิษย์เก่านั้นมีการใช้งานอยู่ในแทบทุกสถาบันการศึกษา ข้อมูลของสมาชิกนั้นประกอบด้วยข้อมูลที่เป็นส่วนตัวที่จะต้องได้รับการปกป้องมิให้ข้อมูลนั้นเกิดการรั่วไหล ซึ่งหากลองค้นบนอินเทอร์เน็ตจะพบว่ามีรายชื่อสมาชิกศิษย์เก่าบางท่านที่ถูกค้นหาพบ ข้อมูลที่พบเหล่านี้ได้สร้างความไม่ปลอดภัยให้กับตัวสมาชิกศิษย์เก่า ทำให้เกิดข้อสงสัยว่าระบบบริการข้อมูลสมาชิกศิษย์เก่าที่ใช้งานอยู่มีมาตรฐานในการรักษาความเป็นส่วนตัวของข้อมูลสมาชิกอย่างไร จะมั่นใจได้อย่างไรว่าระบบสามารถจัดเก็บข้อมูลที่เป็นส่วนตัวของสมาชิกไว้อย่างปลอดภัย เฉพาะผู้ที่มีสิทธิ์เท่านั้นจึงจะสามารถเข้าถึงข้อมูลส่วนบุคคลได้ เป็นเรื่องยากที่จะนำมาตรฐานการรักษาความเป็นส่วนตัว กฎหมายที่มีอยู่ในปัจจุบัน หรือแนวทางปฏิบัติที่เป็นตัวอย่างที่ดีต่างๆ มาปฏิบัติตามหรือเลือกใช้ได้อย่างถูกต้องครบถ้วนได้อย่างสมบูรณ์ เนื่องจากการรักษาความเป็นส่วนตัวนั้นประกอบด้วยรายละเอียดจำนวนมาก จำเป็นที่จะต้องพัฒนาหรือเลือกใช้ซอฟต์แวร์ประเภทนี้โดยผู้ที่มีความรู้ความเข้าใจเพียงพอในการรักษาความเป็นส่วนตัว งานวิจัยนี้ได้เล็งเห็นว่ามีความจำเป็นที่จะต้องรวบรวมความจำเป็นพื้นฐาน ของระบบบริการข้อมูลสมาชิกศิษย์เก่า ออกมาในรูปแบบทั่วไปเพื่อประกอบกับการรักษาเป็นส่วนตัว เพื่อใช้เป็นแนวทางปฏิบัติและเป็นตัวช่วยในการพัฒนาระบบบริการข้อมูลสมาชิกศิษย์เก่า โดยอ้างอิงตามมาตรฐาน กฎหมาย แบบรูปความเป็นส่วนตัว ตัวอย่างวิธีการรักษาความเป็นส่วนตัวที่มีการใช้งานจริงในปัจจุบัน และเทคโนโลยีที่จะมารักษาความเป็นส่วนตัว



ภาพที่ 1.1 ตัวอย่างข้อมูลที่มีการรั่วไหลเมื่อค้นหาด้วยกูเกิล (Google)

ภาพที่ 1.1 แสดงตัวอย่างข้อมูลส่วนบุคคลที่สามารถพบได้เมื่อค้นหาด้วยกูเกิล (Google) ข้อมูลส่วนบุคคลที่ปรากฏได้แก่ วันเกิด หมายเลขโทรศัพท์ ที่อยู่ สถานที่ทำงาน หมายเลขโทรศัพท์ที่ทำงาน และ อื่นๆ ซึ่งข้อมูลเหล่านี้หากมีผู้ไม่หวังดี หรือ ผู้ร้ายนำไปใช้ในทางที่ผิด ย่อมส่งผลเสียและอาจทำให้เจ้าของข้อมูลตกอยู่ในอันตรายได้

1.2. วัตถุประสงค์ของการวิจัย

1.2.1. เพื่อพัฒนาแนวทางเกี่ยวกับความเป็นส่วนตัวสำหรับระบบบริการข้อมูลสมาชิกศิษย์เก่า โดยยึดตามกฎระเบียบในการปกป้องข้อมูลส่วนบุคคลที่ประกาศใช้ในประเทศไทย

1.2.2. แนวทางเกี่ยวกับความเป็นส่วนตัวสำหรับระบบบริการข้อมูลสมาชิกศิษย์เก่าที่พัฒนาขึ้นมานี้จะครอบคลุมถึงเทคโนโลยีที่ใช้ในการปกป้องข้อมูลส่วนบุคคลในปัจจุบัน

1.3. ขอบเขตของการวิจัย

1.3.1. งานวิจัยนี้จะครอบคลุมเฉพาะฟังก์ชันการทำงานทั่วไปของระบบข้อมูลสมาชิกศิษย์เก่า

1.3.2. งานวิจัยนี้จะนำแบบรูปความเป็นส่วนตัวที่มีการพัฒนาก่อนหน้านี้มาใช้ประกอบในการวิจัย

1.3.3. งานวิจัยนี้จะวิเคราะห์และพิจารณาควบคู่กับกฎระเบียบ แนวทางปฏิบัติและมาตรฐานที่จะใช้เพื่อปกป้องข้อมูลส่วนบุคคลในปัจจุบัน

1.3.4. งานวิจัยนี้จะครอบคลุมถึงการพัฒนาแนวทางสำหรับการเชื่อมโยงข้อมูลถึงผู้ให้บริการเสริมที่เป็นบุคคลที่สาม (Third Party)

1.3.5. งานวิจัยนี้ไม่รับประกันความเป็นส่วนตัวได้ทั้งหมดแต่จะทำให้การดูแลความเป็นส่วนตัวดีขึ้นดังนี้

1.3.5.1 เปิดโอกาสและมีแนวทางที่ชัดเจนให้ผู้ใช้งานสามารถระบุความเป็นส่วนตัวของข้อมูลที่มอบให้กับระบบได้

1.3.5.2 อ้างอิงกับกฎหมายในปัจจุบัน จึงทำให้ระบบมีส่วนประกอบที่จะดำเนินการทางด้านความเป็นส่วนตัวตามบัญญัติของกฎหมาย

1.3.5.3 มีแนวทางในการเชื่อมโยงกับผู้ให้บริการเสริมที่เป็นบุคคลที่สาม (Third Party) ที่ชัดเจน

1.4. ประโยชน์ที่คาดว่าจะได้รับ

1.4.1 ผู้พัฒนาระบบบริการข้อมูลสมาชิกศิษย์เก่า มีวิธีการที่ชัดเจน เพื่อรักษาความเป็นส่วนตัว

1.4.2 ทำให้เว็บไซต์บริการข้อมูลสมาชิกศิษย์เก่ามีความน่าเชื่อถือ

1.4.3 ป้องกันผู้ให้บริการการถูกฟ้องร้องเนื่องจากละเมิดความเป็นส่วนตัว

1.4.4 มีแนวทางเพื่อปกป้องความเป็นส่วนตัวในการเชื่อมโยงข้อมูลกับแอปพลิเคชันหรือเว็บไซต์อื่น

1.5. วิธีดำเนินการวิจัย

1.5.1. ศึกษาและรวบรวมฟังก์ชันการทำงานในรูปแบบทั่วไปของระบบบริการข้อมูลสมาชิกศิษย์เก่า

1.5.2. ศึกษาและคัดกรองประเด็นความเป็นส่วนตัวตามข้อกำหนด มาตรฐานแบบรูป และแนวทางปฏิบัติในปัจจุบัน

1.5.3 ศึกษาเทคโนโลยีที่ใช้ในการรักษาความเป็นส่วนตัวสำหรับเว็บแอฟพลิเคชัน

1.5.4. วิเคราะห์องค์ประกอบที่เกี่ยวข้องกับการรักษาความเป็นส่วนตัวในข้างต้นที่ได้กล่าวมา และทำการสังเคราะห์ให้ได้มาซึ่งแนวในการรักษาความเป็นส่วนตัวสำหรับระบบศิษย์เก่า

1.5.5. นำแนวทางในการปกป้องความเป็นส่วนตัว สำหรับระบบบริการข้อมูลสมาชิกศิษย์เก่าที่ได้ไปประเมินระบบอีแอลจีจี (Elgg) เพื่อระบุถึงส่วนที่ยังต้องปรับปรุงเพื่อให้ระบบสามารถรักษาความเป็นส่วนตัวได้ดีมากขึ้น และเพื่อเป็นแนวทางในการนำไปประยุกต์ใช้เป็นระบบบริการข้อมูลสมาชิกศิษย์เก่า พร้อมทั้งนำเสนอรายการของปลั๊กอินที่เกี่ยวข้องซึ่งมีใช้อยู่ในปัจจุบันสำหรับการปกป้องความเป็นส่วนตัว

1.5.6. สรุปผลงานวิจัย

1.6. ลำดับขั้นตอนในการเสนอผลการวิจัย

วิทยานิพนธ์นี้แบ่งเนื้อหาทั้งหมด 5 บท โดยแต่ละบทประกอบไปด้วยเนื้อหาดังต่อไปนี้

บทที่ 1 นำเสนอ ความเป็นมาและความสำคัญของปัญหา วัตถุประสงค์ของการวิจัย ขอบเขตของการวิจัย คำจำกัดความที่ใช้ในการวิจัย ประโยชน์ที่คาดว่าจะได้รับ และวิธีดำเนินการวิจัย

บทที่ 2 อธิบาย

1. ทฤษฎีที่เกี่ยวข้อง เช่น ระบบบริการข้อมูลสมาชิกศิษย์เก่า (Alumni Management System) หลักการความเป็นส่วนตัว (Privacy Principles) ข้อบังคับความเป็นส่วนตัว (Privacy Constraint) เป็นต้น

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง เช่น แนวทางในการรักษาความเป็นส่วนตัว (Privacy Guideline) แบบรูปความเป็นส่วนตัว (Privacy Pattern) การรักษาความเป็นส่วนตัว (Privacy Protection) และ ซอฟต์แวร์ระบบสังคมออนไลน์ (Social Network Software)

บทที่ 3 ประกอบด้วย ภาพรวมและขั้นตอนการดำเนินการวิจัย

บทที่ 4 นำเสนอ วิธีการวิเคราะห์ความเป็นส่วนตัวเซเว่นซี (7C Privacy Analysis Methodology) และ ข้อกำหนดรายละเอียดสิทธิส่วนบุคคล (Privacy Detail Specification)

บทที่ 5 สรุปผลการวิจัย

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1. ทฤษฎีที่เกี่ยวข้อง

2.1.1. ระบบบริการข้อมูลสมาชิกศิษย์เก่า (Alumni Management System)

ระบบบริการข้อมูลสมาชิกศิษย์เก่าเป็นระบบที่พัฒนาขึ้นเพื่อใช้เป็นศูนย์กลางในการประสานงาน และประชาสัมพันธ์ข่าวสารระหว่างสถานศึกษาและศิษย์เก่า ที่สำเร็จการศึกษาในหลักสูตรหรือรุ่นต่างๆ ของสถานบันการศึกษา ตลอดจนใช้เป็นแหล่งข้อมูลศิษย์เก่า นอกจากนั้นแล้วยังเป็นเครื่องมือในการค้นหาข้อมูลสมาชิกศิษย์เก่าและใช้เพื่อติดต่อสื่อสารระหว่างกัน ระบบจะประกอบด้วยความสามารถต่างๆ เช่น การสมัครสมาชิก การจัดการทะเบียนสมาชิก เว็บบอร์ด การจัดการความเป็นส่วนตัวของข้อมูลส่วนบุคคล และระบบจัดส่งอีเมลถึงสมาชิก เป็นต้น เพื่อให้เกิดความเข้าใจอย่างแน่ชัดว่าระบบบริการข้อมูลศิษย์เก่ามีฟังก์ชันการทำงานอะไรบ้างนั้น จึงได้ศึกษาจากเอกสารการออกแบบและพัฒนาระบบจากตัวอย่างการพัฒนาระบบบริการข้อมูลสมาชิกศิษย์เก่า “Alumni Management System” [1] และ “Software Requirements Specification for Larkut.com” [2]

2.1.2. ข้อมูลส่วนบุคคล

สำหรับประเทศไทย การให้ความหมายของข้อมูลส่วนบุคคลปรากฏเป็นครั้งแรกในพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 4 ซึ่งหมายความว่า "ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย" ซึ่งผู้วิจัย [3] ได้รวบรวมความหมายของข้อมูลส่วนบุคคลไว้ทั้งของประเทศไทยและอีกหลายประเทศและทั้งของโออีซีดีว่า “ข้อมูลส่วนบุคคล” หมายความว่า “ข้อความ (Information) ใดๆ อันระบุตัว (Identified) หรืออาจระบุตัว (Identifiable) บุคคล (Individual) ได้” และสำหรับหลักการของการรักษาความเป็นส่วนตัวนั้นยังได้ถูกนำเสนอใน Wikipedia “Privacy” [4] และ “Addressing privacy: matching user requirements to implementation techniques” [5] ซึ่งมีเนื้อหาอธิบาย Anonymity Pseudonymity Unlinkability และ Unobservability

2.1.3. การคุ้มครองข้อมูลส่วนบุคคลในระดับสากล

หลักการในการคุ้มครองข้อมูลส่วนบุคคลในระดับสากลนั้นมีหลายฉบับ ในงานวิจัยของ Yang Wang และ Alfred Kobsa [6] สรุปให้เห็นว่ามีหลักการและประกาศอะไรบ้างที่เกี่ยวข้องกัน ซึ่งได้แสดงในภาพที่ 2.1 สำหรับหัวตารางแนวนอน คือ หลักการในการปกป้องข้อมูลส่วนบุคคลที่ได้ประกาศโดยองค์กรและประเทศต่างๆ เช่น OECD EU APEC เป็นต้น ส่วนหัวตารางในแนวตั้งคือ หลักการพื้นฐานความเป็นส่วนตัวที่เกี่ยวข้องกับประกาศแต่ละฉบับ

Specification / Principle	OECD Guide-lines (OECD, 1980)	EU Directive on Data Protection (EU, 1995)	German Telemedia Law (DE-TML, 2007)	APEC Privacy Framework (APEC-FIP, 2004)	FTC Safe Harbor Principles (FTC, 2000c)	FTC Fair Info Practice (FTC, 2000b)	ACM Principles (USACM, 2006)
Notice/Awareness	X	X	X	X	X	X	X
Minimization							X
Purpose specification	X	X	X	X	X		X
Collection limitation		X	X	X	X		
Use limitation	X	X	X	X	X		X
Onward transfer		X	X		X		
Choice/Consent	X	X	X	X	X	X	X
Access/Participation	X	X	X	X	X	X	X
Integrity/accuracy	X	X	X	X	X	X	X
Security	X	X	X	X	X	X	X
Enforcement/Redress		X	X		X	X	
Anonymity-related principles							
Anonymity							
Pseudonymity		X	X				
Unobservability							
Unlinkability							
Deniability							
Other desirable principles for privacy enhancement							
User preference							
Negotiation							
Seclusion							
Ease of adoption							
Ease of compliance							
Usability							
Responsiveness							

X หมายถึง หลักการพื้นฐานด้านความเป็นส่วนตัวในแนวนอนเกี่ยวข้องกับแนวทางการคุ้มครองข้อมูลส่วนบุคคลแต่ละฉบับในแนวตั้ง

ภาพที่ 2.1 หลักการความเป็นส่วนตัวที่ปรากฏในแนวทางต่างๆ

2.1.4. การคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย

เนื่องด้วยประเทศไทยใช้แนวทางโออีซีดี (OECD) [7] เป็นแม่แบบในประกาศแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานรัฐ พ.ศ.2553 งานวิจัยนี้จึงมุ่งเน้นไปที่แนวทางที่ประเทศไทยใช้เป็นหลัก ซึ่งหลักการของ โออีซีดี (OECD) นั้นเป็นที่ยอมรับและนิยมนำไปใช้อย่างกว้างขวางทั่วโลกตั้งแต่ปี1980 [8] ซึ่งสังเกตได้จากหลายๆ งานวิจัยมีที่อ้างอิงถึง ส่วนประกาศของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวทางปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานรัฐ พ.ศ. 2553 [9] มีเนื้อความดังต่อไปนี้

2.1.4.1 หลักข้อจำกัดในการเก็บรวบรวมข้อมูล คือ ต้องชอบด้วยกฎหมายและต้องใช้วิธีการที่เป็นธรรมและเหมาะสม โดยเจ้าของข้อมูลรู้เห็น รับรู้ หรือได้รับความยินยอมจากเจ้าของข้อมูล

2.1.4.2 หลักคุณภาพของข้อมูล คือ ข้อมูลที่เก็บรวบรวมนั้นต้องเกี่ยวข้องกับวัตถุประสงค์ที่กำหนดขึ้นว่า “จะนำไปใช้ทำอะไร” และเป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของหน่วยงานตามที่กฎหมายกำหนด นอกจากนั้นข้อมูลดังกล่าวจะต้องถูกต้อง สมบูรณ์ หรือทำให้เป็นปัจจุบันหรือทันสมัยอยู่เสมอ

2.1.4.3 หลักการกำหนดวัตถุประสงค์ในการจัดเก็บ คือ ต้องกำหนดวัตถุประสงค์ว่า ข้อมูลที่มีการเก็บรวบรวมนั้น เก็บรวมรวมไปเพื่ออะไร พร้อมทั้งกำหนดระยะเวลาที่เก็บรวบรวมหรือรักษาข้อมูลนั้น ตลอดจนกรณีที่จำเป็นต้องมีการเปลี่ยนแปลงวัตถุประสงค์ในการเก็บรวบรวมข้อมูลเช่นว่านั้น ไว้ให้ชัดเจน

2.1.4.4 หลักข้อจำกัดในการนำไปใช้ คือ ข้อมูลส่วนบุคคลนั้น จะต้องไม่มีการเปิดเผย ทำให้มี หรือปรากฏในลักษณะอื่นใด ซึ่งไม่ได้กำหนดไว้โดยชัดแจ้งในวัตถุประสงค์ของการเก็บรวบรวมข้อมูล เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูล หรือโดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย

2.1.4.5 หลักการรักษาความมั่นคงปลอดภัยข้อมูล คือ จะต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม เพื่อป้องกันความเสี่ยงภัยใดๆ ที่อาจจะทำให้ข้อมูลนั้นสูญหาย เข้าถึง ทำลาย ใช้ ดัดแปลงแก้ไข หรือเปิดเผยโดยมิชอบ

2.1.4.6 หลักการเปิดเผยข้อมูล คือ ควรมีการประกาศนโยบายฯ ให้ทราบโดยทั่วกัน หากมีการปรับปรุงแก้ไข หรือพัฒนาแนวนโยบายหรือแนวปฏิบัติที่เกี่ยวกับข้อมูลส่วนบุคคล ก็ควรเปิดเผยหรือประกาศไว้ให้ชัดเจน รวมทั้งให้ข้อมูลใดๆ ที่สามารถระบุเกี่ยวกับหน่วยงานของรัฐผู้ให้บริการ ที่อยู่ ผู้ควบคุมข้อมูลส่วนบุคคล ด้วย

2.1.4.7 หลักการมีส่วนร่วมของบุคคล คือ ให้บุคคลซึ่งเป็นเจ้าของข้อมูลได้รับแจ้งหรือยืนยันจากหน่วยงานของรัฐที่เก็บรวบรวมหรือจัดเก็บข้อมูลทราบว่า “หน่วยงานของรัฐนั้นๆ ได้รวบรวมข้อมูลหรือจัดเก็บข้อมูลส่วนบุคคลดังกล่าวหรือไม่ ภายในระยะเวลาที่เหมาะสม”

2.1.4.8 หลักความรับผิดชอบ คือ ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

2.1.5. **เครื่องหมายแสดงความน่าเชื่อถือ** (Trustmark/Seal Program)

แม้ว่าเจ้าของเว็บไซต์จะมีการจัดทำนโยบายการคุ้มครองความเป็นส่วนตัวแล้ว แต่ลูกค้าอาจยังไม่แน่ใจว่าเจ้าของเว็บไซต์จะปฏิบัติตามนโยบายที่แสดงไว้ ดังนั้นเพื่อสร้างความน่าเชื่อถือให้เกิดกับลูกค้าผู้ใช้บริการ เจ้าของเว็บไซต์จึงแสวงหาวิธีการที่จะทำให้ลูกค้าที่เข้ามาใช้บริการเห็นว่าตนได้ปฏิบัติตามนโยบายที่ได้ประกาศไว้อย่างแน่นอน วิธีหนึ่งที่นิยมใช้กันอย่างมาก คือการใช้เครื่องหมายแสดงความน่าเชื่อถือ ซึ่งจะทำหน้าที่รับรองและสร้างความน่าเชื่อถือให้กับเว็บไซต์ว่า นโยบายการคุ้มครองความเป็นส่วนตัวของเว็บไซต์ดังกล่าวได้ผ่านการตรวจสอบมาตรฐานจากองค์กรหรือผู้ให้การรับรองเครื่องหมายนั้นแล้ว ปัจจุบันมีหลายองค์กรที่เปิดให้บริการรับรองเครื่องหมายดังกล่าว เช่น ทรัสต์อี (TRUSTe) [10] หรือ บีบีบีออนไลน์ (BBBOnline) [11] เป็นต้น

2.2. งานวิจัยที่เกี่ยวข้อง

2.2.1. การปกป้องข้อมูลส่วนบุคคล (Privacy Protection)

Privacy Enhancing Technologies (PETs) [12] เป็นชุดของเครื่องมือ แอฟลิเคชัน วิธีการ และกลไกในการปกป้องข้อมูลส่วนบุคคล เช่น anonimizer tools, pseudonymizer tools, track and evidence erasers และ encryption tools เป็นต้น

Using Privacy Process Patterns for Incorporating Privacy Requirements into the System Design Process [13] Kalloniatis และคณะนำเสนอแบบรูปทั้งแปดเพื่อใช้ในการปกป้องความเป็นส่วนตัว นั้นสามารถจับคู่กับ Privacy Enhancing Technologies (PETs) ต่างๆได้ ตามรูปภาพที่ 2.2 แบบรูปที่ Kalloniatis ได้นำเสนอนั้นได้แก่ identification, authentication, authorization, data protection, anonymity, pseudonymity, unlinkability, และ unobservability

	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	X			
Unobservability			X	X	X												X	X	X			X	X	X	X	X	X	X

X หมายถึง แบบรูปความเป็นส่วนตัวในแนวนอนใช้ PETs เพื่อรักษาความเป็นส่วนตัว

ภาพที่ 2.2 การจับคู่ระหว่าง PETs กับแบบรูปทั้งแปดของ Kalloniatis

Privacy on the Web: facts, challenges, and solutions [14] ซึ่ง Bouguettaya และคณะได้นำเสนอเทคโนโลยีที่จะใช้ในการปกป้องความเป็นส่วนตัวได้แก่ VPN, Firewall, PGP, Onion routing และ อื่นๆ

Addressing privacy: matching user requirements to implementation techniques [5] ซึ่ง Kavakli และคณะได้นำเสนอความต้องการพื้นฐานด้านความเป็นส่วนตัวที่ต้องคำนึงถึงในขั้นตอนการออกแบบและพัฒนาระบบ และยังได้นำเสนอเทคโนโลยีเพื่อทำให้ระบบสามารถรักษาความเป็นส่วนตัวได้ ได้แก่ Anonimizer, Crowds, Onion routing เป็นต้น

2.2.2. Social Network Software

A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements [15] ซึ่ง Deng และคณะได้นำเสนอ Misuse cases of social network 2.0 for privacy requirements and suggested mitigation strategies and techniques บนพื้นฐาน LINDDUN Privacy Threat Modeling Methodology และ Privacy Enhancing Technologies (PETs).

Open Source Web Content Management Systems to Build Social Network Websites [16] ซึ่ง Omar และคณะได้ประเมินระบบ Web Content Management System (WCMSs) และจัดให้อีแอลจีจี (Elgg) เป็นตัวเลือกหมายเลขลำดับที่สองที่น่าสนใจ

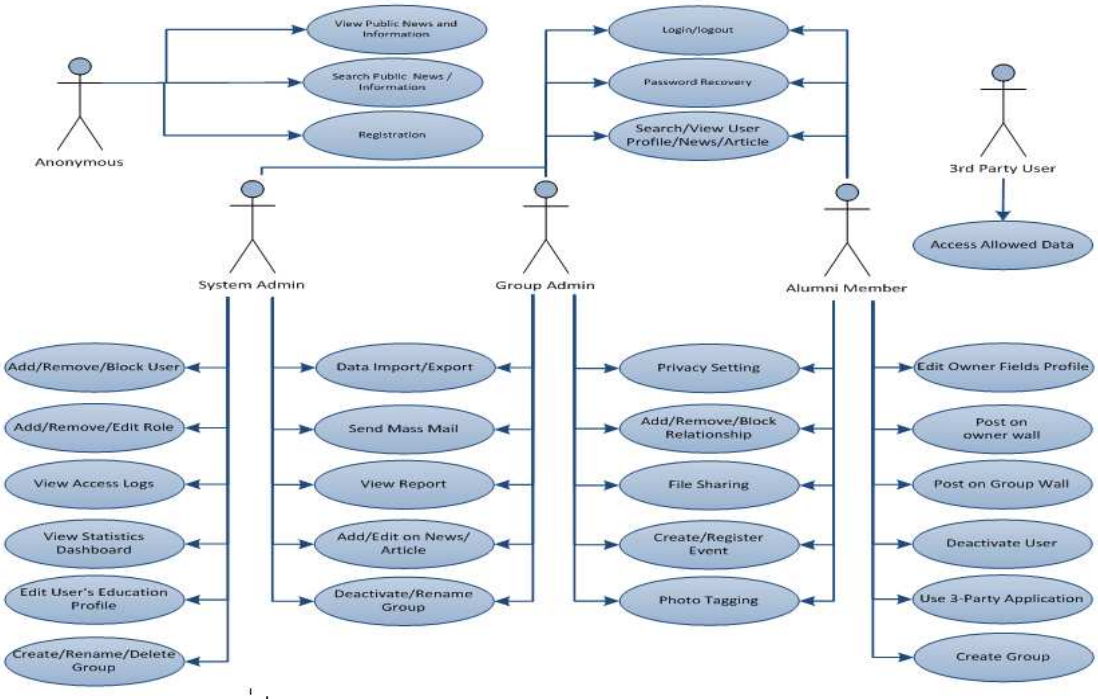
An on-line collaborative data management system [17] ซึ่ง Curry และคณะ ได้ให้เหตุผลว่าทำไม อีแอลจีจี (Elgg) ถึงเหมาะสมที่จะถูกนำมาใช้ เพราะ อีแอลจีจี (Elgg) มีระบบ Access Control ที่มีประสิทธิภาพสามารถควบคุม การเข้าถึงได้ทุกชิ้นข้อมูลส่วนบุคคล และนอกจากนั้นโครงสร้างข้อมูลของอีแอลจีจี (Elgg) นั้นมีความยืดหยุ่นสูง

บทที่ 3

วิธีดำเนินการวิจัย

งานวิจัยนี้นำเสนอแนวทางในการรักษาความเป็นส่วนตัวของระบบบริการข้อมูลสมาชิกศิษย์เก่า โดยมีวิธีดำเนินการวิจัยดังต่อไปนี้

1. ศึกษาและรวบรวมฟังก์ชันการทำงานในรูปแบบทั่วไปของระบบบริการข้อมูลสมาชิกศิษย์เก่า เนื่องจากฟังก์ชันการทำงานของระบบบริการข้อมูลสมาชิกศิษย์เก่าขึ้นอยู่กับแต่ละสถาบันการศึกษาหรือองค์กร ว่าต้องการให้ระบบนั้นมีความสามารถทำอะไรได้บ้าง ดังนั้นก่อนที่จะทำการวิเคราะห์และสังเคราะห์ ให้ได้มาซึ่งแนวทางในการรักษาความเป็นส่วนตัว จึงจำเป็นต้องรู้ฟังก์ชันการทำงานในรูปแบบทั่วไปของระบบเสียก่อน โดยศึกษาจากเว็บไซต์ CAPTERA [18] ซึ่งเป็นเว็บไซต์ที่ได้รับความนิยมในการให้คำแนะนำการเลือกใช้ซอฟต์แวร์ต่างๆ (Software shopping guide) และ Software Detail Design [2] [3] ที่ปรากฏในอินเตอร์เน็ต เมื่อศึกษาพบว่าผู้ใช้งานระบบบริการข้อมูลสมาชิกศิษย์เก่านั้นมีฟังก์ชันการทำงานหลากหลาย ซึ่งได้แสดงไว้ในรูปภาพที่ 3.1 ผู้วิจัยพบว่าสามารถจัดกลุ่มผู้ใช้งานระบบได้แก่ ผู้ใช้งานทั่วไป (Anonymous User) สมาชิกระบบ (Alumni) เจ้าหน้าที่ดูแลกลุ่มและข้อมูล (Group/Data Administrator) ผู้ดูแลระบบ (System Administrator) บุคคลที่สาม (Third-party User)



ภาพที่ 3.1 ฟังก์ชันการทำงานของระบบข้อมูลสมาชิกศิษย์เก่า

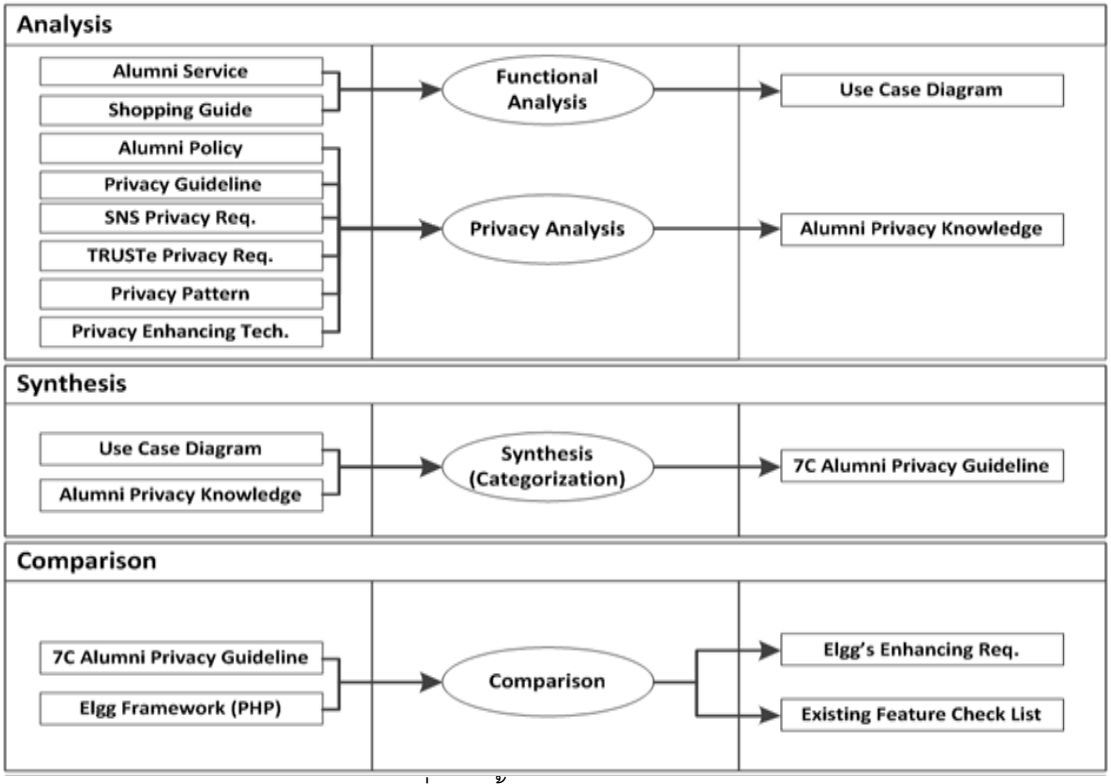
2. ศึกษาและคัดกรองประเด็นความเป็นส่วนตัวตามข้อกำหนด มาตรฐาน แบบรูปความเป็นส่วนตัว แนวทางปฏิบัติในปัจจุบัน และกฎหมายในการรักษาความเป็นส่วนตัว กฎระเบียบและมาตรฐานเหล่านี้ ต้องถูกเอามาพิจารณาประกอบเพื่อให้ระบบบริการข้อมูลสมาชิกศิษย์เก่ามีความน่าเชื่อถือด้านการรักษาความเป็นส่วนตัว

3. ศึกษาเทคโนโลยีที่ใช้ในการรักษาความเป็นส่วนตัว

4. วิเคราะห์องค์ประกอบที่เกี่ยวข้องกับการรักษาความเป็นส่วนตัวในตามที่ได้กล่าวมา และทำการสังเคราะห์ให้ได้มาซึ่งแนวในการรักษาความเป็นส่วนตัวสำหรับระบบบริการข้อมูลสมาชิกศิษย์เก่า

5. นำแนวทางในการปกป้องความเป็นส่วนตัวสำหรับระบบบริการข้อมูลสมาชิกศิษย์เก่าที่ได้ไปประเมินระบบอีแอลจีจี (Elgg) ระบุหาส่วนที่จะต้องปรับปรุงเพื่อให้ระบบสามารถรักษาความเป็นส่วนตัวได้ดีมากขึ้นและเพื่อเป็นแนวทางในการนำไปประยุกต์ใช้เป็นระบบบริการข้อมูลสมาชิกศิษย์เก่า พร้อมทั้งนำเสนอรายการของปลั๊กอินที่เกี่ยวข้องและมีใช้งานอยู่ในปัจจุบันสำหรับการปกป้องความเป็นส่วนตัว

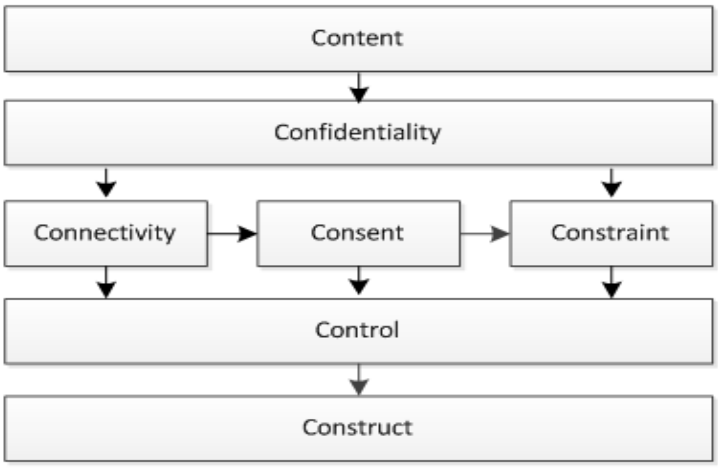
ในการทำงานวิจัยเพื่อให้ได้มาซึ่งแนวทางในการรักษาความเป็นส่วนตัวสำหรับระบบบริการข้อมูลสมาชิกศิษย์เก่านั้น สามารถสรุปให้เห็นสามขั้นตอนหลัก ซึ่งได้แสดงไว้ใน ภาพที่ 3.2 โดย เริ่มต้นจากการศึกษารวบรวมข้อมูลที่เกี่ยวข้องกับการรักษาความเป็นส่วนตัวของระบบบริการข้อมูลสมาชิกศิษย์เก่า ตามที่ได้กล่าวมาแล้วข้างต้น เมื่อรวบรวมข้อมูลต่างๆ เสร็จแล้ว จึงทำการวิเคราะห์เพื่อให้ได้มาซึ่งฟังก์ชันการทำงานพื้นฐานของระบบบริการข้อมูลสมาชิกศิษย์เก่าและความรู้เกี่ยวกับการรักษาความเป็นส่วนตัว เมื่อเข้าสู่ขั้นตอนที่สองคือการสังเคราะห์องค์ความรู้ที่ได้จากขั้นตอนแรก มาเป็นแนวทางสำหรับการรักษาความเป็นส่วนตัวของระบบบริการข้อมูลสมาชิกศิษย์เก่าผ่านการสังเคราะห์ ในขั้นตอนนี้จะทำการจัดหมวดหมู่ (Categorization) ให้ได้มาซึ่งวิธีการวิเคราะห์ความเป็นส่วนตัวเซเว่นซี (7C Privacy Analysis Methodology) ซึ่งจะกล่าวถึงในบทต่อไป ส่วนขั้นตอนลำดับสุดท้ายนั้น คือ การนำแนวทางการรักษาความเป็นส่วนตัวที่ได้ซึ่งอยู่ในรูปแบบเอกสาร Privacy Detail Specification (PDS) มาประเมินผลระบบอีแอลจีจี (Elgg) เพื่อให้ได้มาซึ่งรายการที่ต้องปรับปรุงในการรักษาความเป็นส่วนตัวเพื่อนำไปประยุกต์ใช้เป็นระบบบริการข้อมูลสมาชิกศิษย์เก่า พร้อมกับนำเสนอปลั๊กอินที่เกี่ยวข้องกับความเป็นส่วนตัวที่มีใช้อยู่ในปัจจุบัน



ภาพที่ 3.2 ขั้นตอนการทำงานวิจัย

บทที่ 4
วิธีการวิเคราะห์ความเป็นส่วนตัวแบบเซเว่นซี

งานวิจัยนี้มีวัตถุประสงค์เพื่อสร้างแนวทางในการรักษาความเป็นส่วนตัวสำหรับระบบบริการข้อมูลสมาชิกศิษย์เก่า โดยยึดตามกฎระเบียบในการปกป้องข้อมูลส่วนบุคคลที่มีประกาศใช้ในประเทศไทยตามแนวทางของโออีซีดี (OECD) แนวทางปฏิบัติในการปกป้องข้อมูลส่วนบุคคลทั้งที่ปรากฏในงานวิจัยต่างๆ และเทคโนโลยีที่ใช้ในการปกป้องข้อมูลส่วนบุคคลในปัจจุบัน ผู้วิจัยเล็งเห็นว่า การรักษาความเป็นส่วนตัวนั้นเป็นเรื่องที่มีความซับซ้อน อยากสำหรับผู้ที่มีความรู้ไม่เพียงพอ จึงได้พยายามคิดหาวิธีทำให้การทำงานเกี่ยวกับเรื่องความเป็นส่วนตัวสามารถทำงานได้ง่ายมากขึ้น โดยเลือกคำในภาษาอังกฤษที่มีความหมายสอดคล้องตามขั้นตอนในการวิเคราะห์ความเป็นส่วนตัวที่ผู้ทำงานวิจัยได้รวบรวมและศึกษามา ผู้วิจัยประสงค์ให้ผู้ที่มีความรู้ด้านการรักษาความเป็นส่วนตัวไม่มากนัก สามารถจำหลักการได้ง่ายขึ้นตามขั้นตอนวิธีทั้งเจ็ดขั้นตอนดังต่อไปนี้ ซึ่งสามารถอธิบายเป็นความสัมพันธ์ได้ดังภาพที่ 4.1 และจะได้กล่าวถึงแต่ละขั้นตอนในรายละเอียดต่อไป



ภาพที่ 4.1 ขั้นตอน 7C Privacy Analysis Methodology

4.1. **เนื้อหา** (Content)

ความหมายของ Content นั้นได้ให้ความหมายไว้ใน Wikipedia “Web content” [19] ว่า “"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” และขั้นตอนในการรวบรวมและทำความเข้าใจทุกๆ เนื้อหาในระบบ ทุกเนื้อหาในระบบต้องถูกนำมาพิจารณาในขั้นตอนนี้ รายการของเนื้อหานั้นสามารถศึกษาได้จาก Use case หรือ Software requirement specification อย่างไรก็ตามเพื่อให้ง่าย รายการของเนื้อหานั้นสามารถถอดได้จากหน้าจอของเว็บไซต์หรือรายงานต่างๆ และงานวิจัยนี้จะศึกษาและยกตัวอย่างการทำงานของหน้า Profile เนื่องด้วยเป็นส่วนที่สัมพันธ์โดยตรงกับข้อมูลส่วนบุคคลและความเป็นส่วนตัว ตารางที่ 4.1 นั้นเป็นตัวอย่างข้อมูลเนื้อหาของระบบฐานข้อมูลสมาชิกศิษย์เก่า โดยเนื้อหาแต่ละส่วนที่ได้จากหน้าจอหรือรายงานต่างๆ นั้นมีความสัมพันธ์ไปถึงว่าใครเป็นผู้ใช้งานเนื้อหาส่วนนั้นๆ ซึ่งได้แสดงไว้ในแถว User ตัวอย่างเช่น ผู้ที่ใช้งานหน้า My profile คือ ตัวศิษย์เก่าเอง (Alumni) ผู้ที่ใช้งานหน้า Another profile ก็คือสมาชิกศิษย์เก่าคนอื่นๆ ที่ไม่ใช้เจ้าของข้อมูล เห็นได้ว่าเนื้อหาในสวนต่างๆนั้น ผู้ที่มีสิทธิ์เท่านั้นจึงสามารถใช้งานได้ตามวัตถุประสงค์ในแถว Purpose of used

ตารางที่ 4.1 เนื้อหาในหน้าจอระบบข้อมูลสมาชิกศิษย์เก่า

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

4.2. **ความลับ** (Confidentiality)

ส่วนนี้เป็นการระบุว่าเนื้อหาใดจากขั้นตอนก่อนหน้านี้เป็นข้อมูลส่วนบุคคลบ้าง ซึ่งระบบจะต้องปกป้องคุ้มครองข้อมูลส่วนบุคคลเหล่านี้ ผู้วิจัยได้เลือกใช้คำว่าคอนฟิเดนเชียล

เพราะข้อมูลส่วนบุคคลนั้นจะต้องได้รับการรักรักษาความลับ การรักษาความลับเป็นคุณสมบัติที่สำคัญสำหรับข้อมูลส่วนบุคคล คำว่าคอนฟิเดนเชียล ที่ผู้วิจัยนำมาเป็นส่วนหนึ่งในกระบวนการเซเว่นซีนี้เจาะจงหมายถึงการรักษาความลับสำหรับข้อมูลส่วนบุคคล ตัวอย่างเช่น ผู้ใช้งานระบบไม่ต้องการให้ข้อมูลส่วนตัวถูกเปิดเผยไปสู่บุคลที่ผู้ใช้งานระบบที่ไม่ได้ให้ความยินยอม นั้นเป็นตัวอย่างหนึ่งที่ระบบสามารถเปิดเผยข้อมูลส่วนบุคคลได้โดยต้องคำนึงถึงว่าข้อมูลส่วนบุคคลนั้นๆ เป็นความลับ เฉพาะบุคลที่เจ้าของข้อมูลอนุญาตให้เข้าถึงได้เท่านั้น สำหรับข้อมูลส่วนบุคคลนั้น US, UK, COPPA, EU ได้กำหนดว่าข้อมูลใดบ้างเป็นข้อมูลส่วนบุคล “Personal Data” [20] สำหรับ Personal Indentifiable Information (PII) นั้นก็ถูกระบุไว้ใน “Personally identifiable information” [21] และ [22] เมื่ออ้างอิงตามข้อมูลส่วนบุคคลที่ได้มีการระบุไว้ดังกล่าวจะสามารถชี้ได้ว่าข้อมูลใดบ้างเป็นข้อมูลส่วนบุคคลที่ต้องได้รับการรักษาให้เป็นความลับ ซึ่งจะถูกเปิดเผยก็ต่อเมื่อได้รับความยินยอมจากเจ้าของข้อมูล ซึ่งเป็นเรื่องสำคัญที่ต้องทำความเข้าใจในความแตกต่างระหว่าง ความเป็นส่วนตัวและความลับ ซึ่งมีผู้ที่เขียนไว้ได้เข้าใจง่ายใน “Do you know the difference between Privacy and Confidential ?” [23] ตัวอย่างข้อมูลส่วนบุคคลซึ่งเป็นความลับนั้นได้แสดงในตารางที่ 4.2 ซึ่งแสดงให้เห็นว่าเนื้อหาใดๆบ้างปรากฏว่าเมื่อข้อมูลส่วนบุคคลอยู่

ตารางที่ 4.2 รายการข้อมูลส่วนบุคคลในเนื้อหา

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					

อักษร e หมายถึงข้อมูลส่วนบุคคลปรากฏในเนื้อหาหมายเลขต่างๆ เช่น Cte#1 Cte#2

4.3. **การเชื่อมโยง** (Connectivity)

การเปิดเผยข้อมูลนั้นเป็นส่วนหนึ่งที่สำคัญการรักษาและปกป้องข้อมูลส่วนบุคคล เนื่องด้วยจะประกอบด้วยขั้นตอนการเข้าถึงข้อมูลส่วนบุคคล ซึ่งต้องถูกควบคุมเพื่อไม่ให้ข้อมูลส่วนบุคคลเกิดการรั่วไหลหรือบุคคลที่ไม่มีสิทธิ์สามารถเข้าถึงและนำข้อมูลไปใช้ได้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล คำว่าคอนเนคชั่น สามารถชี้ให้เห็นถึงการเชื่อมโยงของข้อมูลส่วนบุคคล ว่าข้อมูลเหล่านั้นถูกเปิดเผยไปสู่ผู้ใช้อื่นหรือสู่สาธารณะอย่างไร ขั้นตอนนี้จะนำรายการเนื้อหาความลับในขั้นตอนก่อนหน้านี้ มาหาความสัมพันธ์กับฟังก์ชั่นการทำงานของระบบในยูสเคสว่ามีฟังก์ชันการทำงานใดใช้งานข้อมูลที่เป็นเนื้อหาคอนฟิเดนเชียลบ้างและมีสิทธิ์การใช้งานข้อมูลส่วนบุคคลต่างๆ ตามเนื้อหาแต่ละส่วนอย่างไรบ้าง ซึ่งได้แสดงในตารางที่ 4.3

ตารางที่ 4.3 **การใช้งานข้อมูลส่วนบุคคลในแบบ** CRUD

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

ตารางที่ 4.3 การใช้งานข้อมูลส่วนบุคคลในแบบ CRUD (ต่อ)

ID	Content's Name	Confidentiality's Name	C	R	U	D
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		

CRUD ในตารางเป็นตัวย่อซึ่งมีความหมายมาจาก Create Read Update และ Delete a ในตารางหมายถึงการที่ระบบอนุญาตให้ใช้งานได้ ซึ่งเป็นไปตามสิทธ์ CRUD ซึ่งผูกพันไปยังแต่ละชื่อเนื้อหา (Content's Name) ส่วน Confidentiality's Name คือ รายการชื่อของ ข้อมูลส่วนบุคคล

เนื่องด้วยที่ได้กล่าวมาในตอนต้นว่าระบบฐานข้อมูลสมาชิกศิษย์เก่านั้นสามารถแบ่งกลุ่มผู้ใช้งานระบบออกเป็น 5 กลุ่มหลัก ได้แก่ ผู้ใช้งานทั่วไป (Anonymous User) สมาชิกระบบ (Alumni) เจ้าหน้าที่ดูแลกลุ่มและข้อมูล (Group/Data Administrator) ผู้ดูแลระบบ (System Administrator) และบุคคลที่สาม (Third-party User) และในขั้นตอน Content ของเซเว่นซีก่อนหน้านี้ ได้ระบุแล้วว่าผู้ใช้กลุ่มใดบ้างที่สามารถใช้งานเนื้อหาในหน้าจอหรือรายงานต่างๆ ได้ ดังนั้นแล้วรายการ Connectivity ในตารางที่ 4.3 จึงถูกบังคับว่าใครสามารถใช้งานเนื้อหาในหน้าจอหรือรายงานต่างๆ ได้ และConnectivity เหล่านี้ ก็สัมพันธ์ไปถึงความยินยอมการให้ใช้ข้อมูลจากเจ้าของข้อมูลในขั้นตอนเซเว่นซี ในลำดับถัดไป

4.4. การยินยอม (Consent)

การยินยอมเปิดเผยข้อมูลเป็นสิ่งที่สำคัญมากเพราะหากระบบจะเปิดเผยข้อมูลส่วนบุคคลของผู้ใช้งานได้นั้นจะต้องได้รับความยินยอมจากเจ้าของข้อมูลเสียก่อน ซึ่งต้องไปตามกฎระเบียบข้อบังคับที่ว่าผู้ใช้งานสามารถเลือกว่าจะเปิดเผยข้อมูลหรือไม่ให้บุคคลหรือกลุ่มบุคคลใดๆ ได้ จากขั้นตอนการทำงานที่แล้วทำให้รู้ว่ามีข้อมูลส่วนบุคคลอะไรบ้างอยู่ที่ใด ในขั้นตอนนี้จะนำข้อมูลส่วนบุคคลที่ได้ดังกล่าวมาพิจารณาต่อและให้รายละเอียดว่าระบบจะเปิดโอกาสให้ผู้ใช้งานสามารถควบคุมการเปิดเผยหรือการใช้งานข้อมูลส่วนตัวหรือเฉพาะกลุ่มอย่างไรบ้าง

ฟังก์ชันการทำงานสำหรับการตั้งค่าการเปิดเผยข้อมูลนั้นเป็นเรื่องที่ละเอียดอ่อนต่อผู้ใช้งาน หากฟังก์ชันการตั้งค่านั้นละเอียดมากเกินไปจะทำให้ผู้ใช้งานตั้งค่าการเปิดเผยข้อมูลตัวเองได้ยาก แต่ถ้าฟังก์ชันนี้มีการตั้งค่าที่ไม่ละเอียดหรือเปิดโอกาสให้เลือกตั้งค่าได้น้อยก็อาจไม่ตอบสนองผู้ใช้งานได้ดีหรือเพียงพอตามข้อระเบียบบังคับหรือกฎหมายที่ได้กล่าวมาแล้ว ซึ่งก็อาจทำให้ผู้ใช้งานไม่อยากใช้งานระบบต่อไปก็เป็นไปได้ซึ่งได้บรรยายไว้ใน “Patterns to Support the Development of Privacy Policies” [24] หากการใช้ข้อมูลบนความยินยอมของผู้ใช้เป็นไปไม่ได้อย่างเหมาะสม การยินยอมให้ผู้ใช้งานมีโอกาสตั้งค่าความยินยอมได้นั้นได้แสดงไว้ในตารางที่ 4.4

ตารางที่ 4.4 **ข้อมูลส่วนบุคคลที่ระบบอนุญาตให้เจ้าของข้อมูลตั้งค่าความยินยอม**

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		

อักษร t หมายถึง Toggle เพื่ออนุญาตให้ผู้ใช้งานมีโอกาสตั้งค่าความยินยอมได้

4.5. **ข้อบังคับ** (Constraint)

ในการพัฒนาระบบที่มีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคล ผู้พัฒนาระบบมีความจำเป็นอย่างมาก ที่จะต้องศึกษาเพื่อให้เกิดความเข้าใจระเบียบและข้อบังคับต่างๆ ที่เกี่ยวข้องกับการใช้งานข้อมูลส่วนบุคคล เนื่องด้วยบุคคลใดๆ ย่อมมีสิทธิ์ที่ปิดหรือเปิดเผยข้อมูลของตนเองได้ ซึ่งเป็นไปตามความคุ้มครองของกฎหมาย ดังนั้นแล้วผู้พัฒนาระบบจะต้องคำนึงถึง ระเบียบ หรือกฎหมายที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เพื่อจะได้ไม่ทำผิดกฎหมายหรือระเบียบข้อบังคับต่างๆ ซึ่งจะมีผลโดยตรงต่อความน่าเชื่อถือและความถูกต้องของระบบที่กำลังพัฒนาอยู่นั้นเอง ตัวอย่างของกฎหมายในประเทศไทย เช่น ประกาศกระทรวงฯ [9] ซึ่งได้ยึดตามแนวทางของ โออีซีดี (OECD) [7] ผู้วิจัยได้แสดงข้อบังคับต่างในตารางที่ 4.5

ตารางที่ 4.5 ข้อบังคับความเป็นส่วนตัวที่ผู้พัฒนาระบบจะต้องคำนึงถึง

ID	Name	Source	Constraint Detail
1	Collection Limit	OECD	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. [25]	The purpose associated with personal information shall have consent of the donor of personal information
10	Data Retention	TRUSTe [10]	The time period of retention PII, How log system will retain that information.

ตารางที่ 4.5 ข้อบังคับความเป็นส่วนตัวที่ผู้พัฒนาระบบจะต้องคำนึงถึง (ต่อ)

ID	Name	Source	Constraint Detail
11	Third Party and Transborder	Skinner et al. [26]	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.

4.6. **ตัวควบคุม** (Control)

จะใช้วิธีอย่างไรในการควบคุมเพื่อรักษาข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามข้อกำหนด ระเบียบข้อบังคับที่ได้จากขั้นตอนก่อนหน้า ผู้วิจัยพบว่า LINDDUN Framework [15] นั้นมีความเหมาะสมที่จะนำมาใช้ควบคู่กับแนวทางในการควบคุมอื่น เช่น Kumari ‘s requirement analysis for privacy in social network [27] และ Intel ‘s privacy requirements and recommendations [28] ใน LINDDUN นั้นแบ่งการรักษาความความเป็นส่วนตัวโดยควบคุมที่ 4 แบบ คือ Entity (E) Data Store (DS) Data Flow(DF) และ Process (P) ผู้วิจัยได้ทำการจับคู่ LINDDUN กับแบบรูปความเป็นส่วนตัวด้วย [13] ซึ่งได้ดังแสดงในตารางที่ 4.6

ตารางที่ 4.6 การจับคู่ข้อบังคับและแบบรูปกับ LINDDUN

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 Disclosure	Confidentiality		x	x	x	Authentication Authorization Identification Data Protection
Content Unawareness	Content awareness	x				OECD & TRUSTe
Policy/Consent Noncompliance	Policy and Consent compliance	x	x	x	x	OECD & TRUSTe

สำหรับการควบคุมนั้น หลังจากได้ตารางที่ 4.6 เพื่อให้ระบบสามารถรักษาความส่วนตัวเป็นไปตามข้อกำหนด ระเบียบข้อบังคับที่ได้จากขั้นตอนก่อนหน้านั้น ผู้วิจัยได้รวบรวมรายละเอียดการควบคุมจากต่างๆจาก LINDDUN Framework [15] ซึ่งได้นำเสนอการควบคุมสำหรับระบบเครือข่ายสังคมออนไลน์ ในการควบคุมที่ส่วนต่างๆ คือ Entity (E) Data Store (DS) Data Flow(DF) และ Process (P) จาก Kumari 's requirement analysis for privacy in social network [27] และจาก Intel 's privacy requirements and recommendations [28] ออกมาเป็นตารางควบคุม ซึ่งได้แสดงไว้ในตารางที่ 4.7 เพื่อใช้ควบคุมความเป็นส่วนตัว เช่น Collection limit Data Qualityเป็นต้น และแสดงรายละเอียดการควบคุมในตารางโดยแบ่งตาม Entity (E) Data Store (DS) Data Flow(DF) และ Process (P)

ตารางที่ 4.7 รายการควบคุม

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.

ตารางที่ 4.7 รายการควบคุม (ต่อ)

ID	Type	How to control software design and development.
		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.

ตารางที่ 4.7 รายการควบคุม (ต่อ)

ID	Type	How to control software design and development.
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.

ตารางที่ 4.7 รายการควบคุม (ต่อ)

ID	Type	How to control software design and development.
16	Unobservability	Data Store) Use sufficient access control and information hiding techniques. Data Flow) Covert channel and steganography can be used to protect privacy.

4.7. **วิธีการ** (Construct)

ขั้นตอนนี้เป็นการเลือกเทคโนโลยีที่นำมาใช้จริง เพื่อทำให้การควบคุมในขั้นตอนก่อนหน้านี้เกิดขึ้นจริงได้ จากตารางของ Kalloniatis ในบทก่อนหน้านี้แสดงให้เห็นว่าเมื่อสามารถระบุ Control ได้ก็จะสามารถจับคู่ไปหา Privacy Enhancing Technologies (PETs) ได้ [12] [15] ตัวอย่างที่นำเสนอในตารางที่ 4.8 ได้แก K-anonynity [15] , Tor [29] เพื่อใช้สร้างระบบขึ้นมาจริง หลังจากได้มีการระบุสิ่งที่จะต้องควบคุมต่างๆในขั้นตอนก่อนหน้านี้ การเลือกใช้เทคโนโลยีเพื่อนำมาใช้จริงนั้นขึ้นอยู่กับหลายปัจจัย เช่น งบประมาณ สถาปัตยกรรมของระบบ ความสามารถในการขยายระบบ ระดับความต้องการในการป้องกัน เวลาที่มี เป็นต้น เรื่องของความปลอดภัยของระบบก็เป็นเรื่องที่สำคัญ เพราะเป็นด่านแรกและด่านสำคัญที่จะใช้ป้องกันผู้บุกรุกได้ ซึ่งก็เป็นหนึ่งในข้อบังคับของ OECD ในหัวข้อเรื่องความปลอดภัยที่ต้องมีเพียงพอเพื่อรักษาความเป็นส่วนตัว งานวิจัย "Privacy on the Web: facts, challenges, and solutions" [14] “Privacy patterns for online interactions” [29] , “Web Contents Protection, Secure Execution and Authorized Distribution” [30] และหนังสือคู่มือระบบอีแอลจีจี “Elgg 1.8 Social Networking” [31] ได้นำเสนอเทคโนโลยีทางด้านความปลอดภัยได้แก่ SSL HTTPS เป็นต้น

ตารางที่ 4.8 การจับคู่กับระหว่าง Control Type กับ 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

ตารางที่ 4.8 การจับคู่กับระหว่าง Control Type กับ Construct (ต่อ)

ID	Name	Short Detail	Control Type
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	Security Safeguards

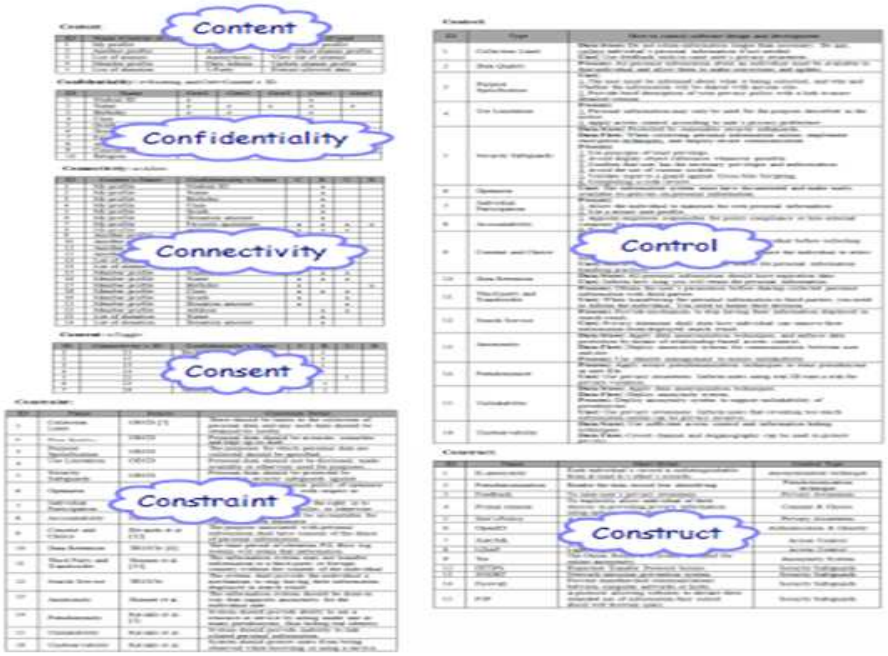
บทที่ 5

ผลการวิจัย

ในบทนี้จะกล่าวถึงผลที่ได้จากการวิจัยตามแนวคิดและวิธีวิจัยในบทที่ 3 ในส่วนของผลการวิจัยนี้ได้แบ่งเป็น 3 ส่วน ได้แก่ Privacy Detail Specification การประเมินระบบอีแอลจีจี และ Primal Consent

5.1 Privacy Detail Specification (PDS)

PDS เป็นเอกสารที่ได้มาจากการทำการวิเคราะห์ความเป็นส่วนตัวตามแนวทาง 7C Privacy Analysis Methodology ซึ่งรายละเอียดนั้นได้อธิบายในบทที่ 4 โดยสรุปแล้ว PDS จะเป็นเอกสารที่บอกถึงตั้งแต่ข้อมูลส่วนบุคคล ที่ปรากฏที่เนื้อหาต่างๆ การใช้งานข้อมูลส่วนบุคคล ความยินยอมการให้ข้อมูล และสิทธิ์ในการประมวลผลข้อมูล กฎระเบียบข้อบังคับ วิธีการควบคุมการใช้ข้อมูลส่วนบุคคล และเทคโนโลยีที่มาสนับสนุนจริงเมื่อพัฒนาระบบ ภาพที่ 5.1 ได้แสดงให้เห็นภาพโดยรวมว่า PDS ประกอบด้วยตารางอะไรบ้าง ได้แก่ Content Confidentiality Connectivity Consent Constraint Control และ Construct ซึ่งรายละเอียดเนื้อหาภายในแต่ละตารางใน PDS สามารถดูรายละเอียดได้ที่ ตาราง 4.1 4.2 4.3 4.4 4.5 4.7 และ 4.8



ภาพที่ 5.1 ตัวอย่างโดยรวม Privacy Detail Specification (PDS)

5.2 การประเมินระบบอีแอลจีจี (Elgg)

ได้ศึกษาคู่มือการใช้งานระบบอีแอลจีจี (Elgg) เวอร์ชัน 1.8 [31] รายการปลั๊กอินที่เกี่ยวข้องกับการรักษาความเป็นส่วนตัวที่แสดงใน “http://community.elgg.org/plugins” [32] และเอกสารที่ผู้วิจัยพบต่างๆออนไลน์ “Comparison of social networking software” [33], “Social Network / Community / Forum Software Comparison Chart” [34] และ “Users, Profiles, and Connections in Elgg” [35] ผู้วิจัยพบว่ามีปลั๊กอินทั้งหมด1653 ปลั๊กอิน 39 ปลั๊กอินเกี่ยวข้องกับการรักษาความเป็นส่วนตัว เมื่อผู้วิจัยประเมินอีแอลจีจีตาม 23 หัวข้อที่ผู้วิจัยสรุปมาจาก PDS พบว่า 4 ฟังก์ชันการทำงานที่เกี่ยวข้องกับการรักษาความเป็นส่วนตัวนั้นไม่ได้สนันสนุนโดยตัวอีแอลจีจีเองและไม่มีปลั๊กอินสนับสนุน ตัวอย่างความสามารถที่ขาดหายไปได้แก่ “Who can look me up” [36] ซึ่งเป็นฟังก์ชั่นการทำงานที่ Facebook มีให้บริการกับผู้ใช้งานระบบในการทำให้ Search Engine ไม่สามารถค้นหาข้อมูลส่วนบุคคลของสมาชิกพบ 9 ปลั๊กอินที่เกี่ยวข้องกับความเป็นส่วนตัวนั้นมีให้ใช้เฉพาะเวอร์ชัน 1.7 ซึ่งสรุปไว้ในตารางด้านล่าง

ตารางที่ 5.1 การประเมินความเป็นส่วนตัวระบบอีแอลจีจีเวอร์ชัน 1.8

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 based 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		

ตารางที่ 5.1 การประเมินความเป็นส่วนตัวอีแอลจีจีเวอร์ชัน 1.8 (ต่อ)

Recommended Privacy related features	Elgg 1.8 Core	Elgg 1.7 Plug-ins	Elgg 1.8 Plug-ins
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 blacklist	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			

ตารางที่ 5.1 การประเมินความเป็นส่วนตัวอีแอลจีจีเวอร์ชัน 1.8 (ต่อ)

Recommended Privacy related features	Elgg 1.8 Core	Elgg 1.7 Plug-ins	Elgg 1.8 Plug-ins
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

5.3 Primal Consent

จากตารางที่ 5.2 แสดงให้เห็นถึงจำนวนตัวอักษรของข้อตกลงหรือสัญญาที่เว็บไซต์ประกาศไว้สำหรับการปกป้องข้อมูลส่วนบุคคล ซึ่งสามารถเข้าค้นหาเพิ่มเติมได้ที่เว็บไซต์ดังกล่าวได้โดยตรงในหัวข้อ Privacy Policy ข้อตกลงเหล่านี้เขียนในภาษากฎหมายซึ่งเข้าใจได้ยากและจะไม่ระบุถึงการใช้งานบนความยินยอมของสมาชิกอย่างละเอียด ซึ่งได้มีการโต้เถียงกันในเรื่องนี้ใน “US congressmen inquire about iOS privacy with Apple, 33 developers” [37] มาบ้างแล้ว ด้วยเนื้อหาการโต้เถียงที่ว่า ผู้ดำรงตำแหน่งหน้าที่ทางการเมืองได้สอบถามผู้พัฒนาแอปพลิเคชันให้ iOS ว่าทำไมแอปพลิเคชันที่พัฒนาขึ้นมาถึงได้เข้าถึงข้อมูล Address book ซึ่งเป็นข้อมูลส่วนบุคคลได้ ผู้ดำรงตำแหน่งหน้าที่ทางการเมืองต้องการทราบว่าแอปพลิเคชัน เอาข้อมูลเหล่านี้ไปใช้ทำอะไร และได้แจ้งเตือนเจ้าของข้อมูลหรือไม่ เนื่องด้วย แอปพลิเคชัน Path ได้ upload ข้อมูล Address book ของผู้ใช้ไปที่เซิร์ฟเวอร์ของตัวเอง โดยไม่ได้รับความยินยอมจากผู้ใช้ Butterfield และ Waxman ได้ส่งจดหมายไปถึง Cook ซึ่งเป็น ซีอีโอของแอปเปิล โดยถามว่า แอปเปิลมีมาตรการการปกป้องข้อมูลส่วนบุคคลที่เพียงพอหรือไม แต่สุดท้ายแอปเปิลทำตัวเหินห่างจากความขัดแย้งโดยระบุว่า การเก็บหรือส่งข้อมูลส่วนบุคคลที่ไม่ได้รับอนุญาตเป็นการละเมิดแนวทางการพัฒนาของตน แอปเปิลสัญญาว่า การที่ซอฟแวร์ต่าง ใน App Store จะสามารถเข้าถึงข้อมูล Address book ของผู้ใช้ได้นั้นจะต้องได้รับการอนุญาตที่ชัดเจนจากผู้ใช้เสียก่อน และแอปเปิลจะเพิ่มความสามารถนี้ใน iOS เวอร์ชันต่อไป

การยินยอมขั้นพื้นฐาน (Primal Consent) ผู้วิจัยเห็นว่าการเก็บรวมรวมข้อมูลของผู้ที่จะสมัครเป็นสมาชิกนั้นควรมีความละเอียดและผูกพันไปถึงเซอร์วิสที่เข้าถึงข้อมูลส่วนบุคล ซึ่งต้องได้รับการยินยอมจากเจ้าของข้อมูลอย่างละเอียดแต่ละชิ้นด้วย แต่จากการที่ Privacy Policy มีจำนวนหน้าที่เยอะมากสำหรับบางเว็บไซต์นั้นอาจเป็นอุปสรรค์ต่อผู้ใช้งานในการอ่านหรืออาจทำให้ผู้อ่านเพิกเฉยการอ่านข้อตกลงดังกล่าว อีกทั้งเนื่องด้วยสัญญาเหล่านี้เป็นภาษากฎหมายที่อ่านจับใจความได้ยาก ผู้วิจัยเห็นว่าควรมีเครื่องมือ อาจจะเป็น ตารางที่จะมาช่วยอธิบายการใช้ข้อมูลส่วนบุคคลที่ละเอียดไปถึงเซอร์วิสที่เข้าถึงข้อมูลส่วนบุคล ซึ่งจะช่วยให้ผู้อ่านเข้าใจได้ง่ายมากขึ้นและน่าเป็นงานที่สนใจในอนาคตที่ควรได้รับการพัฒนา แต่เนื่องด้วยการพัฒนาเครื่องมือที่จะมาใช้อธิบาย การยินยอมขั้นพื้นฐาน อยู่นอกเหนือขอบเขตุของงานวิจัยนี้ จึงได้ เสนอประเด็นไว้เพื่อที่จะได้พัฒนาต่อในอนาคต

ตารางที่ 5.2 จำนวนคำของข้อตกลงจากเว็บไซต์ที่เป็นที่มีชื่อเสียง

Site	AT&T	Facebook	Linked-in	WhatApp	Skype	Ebay	IBM	Myspace	Amazon	Apple	Google+	Twitter	LINE
Words	9089	9325	7330	6397	5213	4000	3967	2821	2692	2415	2240	2151	1903

บทที่ 6
สรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ

6.1. สรุปผลการวิจัย

งานวิจัยนี้ได้พัฒนาวิธีการวิเคราะห์ความเป็นส่วนตัวเซเว่นซี (7C Privacy Analysis Methodology) และเอกสารประกอบเพื่อใช้เป็นแนวทางในการพัฒนาความเป็นส่วนตัว คือ Privacy Detail Specification (PDS) ผู้ทำงานวิจัยคาดหวังว่าสิ่งที่ได้นำเสนอนี้จะสามารถช่วยให้ผู้ที่มีความรู้ไม่มากนักเกี่ยวกับการรักษาความเป็นส่วนตัว จนถึงผู้ที่กำลังพัฒนาระบบข้อมูลสมาชิกศิษย์เก่าสามารถทำความเข้าใจการรักษาความเป็นส่วนตัวได้มากขึ้น โดยมีแนวทางเป็นหลักให้ยึดดังที่ได้นำเสนอมา งานวิจัยนี้ยังได้นำแนวทางที่พัฒนาขึ้นมาประเมินระบบอีแอลจีจี (Elgg) ซึ่งมีประโยชน์สำหรับผู้ที่กำลังมองหา Open Source ซอฟต์แวร์สำหรับการพัฒนาระบบข้อมูลสมาชิกศิษย์เก่า และเพื่อให้อีแอลจีจี (Elgg) ครอบคลุมการปกป้องคุ้มครองความเป็นส่วนตัว งานวิจัยนี้จึงได้นำเสนอรายการของปลั๊กอินที่สนับสนุน ซึ่งมีประโยชน์ช่วยให้ผู้ที่กำลังพัฒนาระบบข้อมูลสมาชิกศิษย์เก่าด้วยอีแอลจีจีสามารถเลือกใช้ปลั๊กอินได้เหมาะสมเพื่อรักษาความเป็นส่วนตัว นอกเหนือจากที่ได้กล่าวมาแล้ว ในงานวิจัยนี้พบว่าการให้ความยินยอมในการเปิดเผยข้อมูลหรือการใช้ข้อมูลสมาชิกนั้น มีการเรียกเก็บข้อมูลสมาชิกตอนที่ทำการสมัครสมาชิกในแบบไม่ละเอียดเจาะจงว่าข้อมูลส่วนบุคคลแต่ละชิ้นจะถูกใช้อย่างไร ซึ่งเป็นการให้สัญญาแบบคร่าวๆ กับสมาชิกในการใช้ข้อมูล ผู้วิจัยพบว่าข้อตกลงหรือสัญญาการใช้ข้อมูลนั้นยาวและยังเป็นภาษาด้านกฎหมายที่เข้าใจได้ยาก จึงเป็นไปได้ยากที่ผู้ใช้งานหรือสมาชิกจะอ่านแล้วเข้าใจได้ทั้งหมด ตัวอย่างเช่น AT&T ที่มีหน้าสัญญาถึง 24 หน้า ผู้วิจัยได้กล่าวถึงการให้ความยินยอมขั้นพื้นฐาน (Primal Consent) ซึ่งกำหนดว่าการเก็บรวมรวมข้อมูลของผู้ที่จะสมัครเป็นสมาชิกนั้นควรมีความละเอียดและผูกพันไปถึงเซอร์วิสที่เข้าถึงข้อมูลส่วนบุคคล ซึ่งต้องได้รับการยินยอมจากเจ้าของข้อมูลอย่างละเอียดแต่ละชิ้นด้วย

6.2. **อภิปรายผล**

แนวทางในการรักษาความเป็นส่วนตัวนั้นได้ถูกนำเสนอออกมาในรูปแบบ PDS ซึ่งเป็นเอกสารที่ช่วยให้ผู้ที่ต้องทำงานเกี่ยวกับเรื่องความเป็นส่วนตัวสามารถมองเห็นภาพโดยรวมของการรักษาความเป็นส่วนตัว ตั้งแต่เนื้อหาในระดับพื้นฐานไปจนถึงเทคโนโลยีที่มาสนับสนุน การนำคำในภาษาอังกฤษทั้งเจ็ดมาร้อยเรียงต่อให้เป็นขั้นตอนนั้นน่าจะทำให้ผู้ที่ใช้งานตระหนักถึงการปกป้องความเป็นส่วนตัวได้มากขึ้นว่ามีองค์ประกอบอะไรบ้างที่ต้องคำนึงถึง และขั้นตอนทั้งเจ็ดของเซเว่นซีนั้นยังทำให้จดจำได้ง่าย ว่าต้องทำอะไรบ้างเพื่อให้ระบบสามารถรักษาความเป็นส่วนตัวได้ดีมากขึ้น

หากเปรียบเทียบว่า 7C ว่าดีกว่าแนวทางอื่นอย่างไร จากที่ผู้วิจัยได้ศึกษามาพบว่าหากเปรียบเทียบกับ Privacy Assessment Guideline อื่นๆ จะเน้นไปที่การวัดให้คะแนนระบบ ว่าสามารถปกป้องความเป็นส่วนตัวได้มากแค่ไหน ซึ่งไม่ได้ให้แนวทางว่าเมื่อจะไปพัฒนาระบบเพื่อให้มีความสามารถในการรักษาความปลอดภัยต้องทำอย่างไร ซึ่งในเอกสารอ้างอิงที่ผู้วิจัยอ้างถึงเช่น TRUSTe ซึ่งเป็นความต้องการของระบบที่ต้องปฏิบัติตามให้ครบ เพื่อให้ได้ใบรองรับรองความเป็นส่วนตัว ก็เห็นได้ว่ามีข้อกำหนดต่างๆ บรรยายไว้เป็นจำนวนมากว่าระบบต้องมีความสามารถอะไรบ้างในการรักษาความเป็นส่วนตัว เซเว่นซีนั้นไม่ได้ดีกว่า TRUSTe ซึ่งในกระบวนการวิเคราะห์เซเว่นซีมีขั้นตอน Constraint เป็นขั้นตอนในการที่รวมความต้องการที่ TRUSTe หรือ ความต้องการทางด้านความเป็นส่วนตัวจากแหล่งอื่นๆ เช่น OECD หรือในงานวิจัยที่ได้อ้างอิงถึงเช่นของ Skinner et หรือ Kavakli et ที่ได้แสดงในตารางที่ 4.5 เพื่อนำข้อจำกัดหรือความต้องการต่างๆ ไปหาวิธีการ และการเทคโนโลยีที่จะนำมาใช้ปกป้องความเป็นส่วนตัวในขั้นตอน Control และ Construct ให้เห็นเป็นรูปธรรมมากขึ้นกว่าการมีเฉพาะข้อกำหนดหรือความต้องการทางด้านความเป็นส่วนตัวต่างๆ ที่พบได้ในแนวทางหรืองานวิจัยต่างๆที่ได้กล่าวมา

6.3. **ข้อเสนอแนะ**

ในขั้นตอนต่อไปควรที่จะต้องพัฒนาระบบข้อมูลสมาชิกศิษย์เก่าขึ้นมาจริงโดยพัฒนาปลั๊กอินขึ้นมาเองสำหรับส่วนที่ยังขาดหายเพื่อให้ระบบสามารถรักษาความเป็นส่วนตัวได้มีประสิทธิผลมากขึ้น

รายการอ้างอิง

[1] Lalita Jarupakwittaya and Hataichanok Naknarong, Alumni Management System. Senior Project, Department of Computer Science, Faculty of Science, Khon Kaen University, 2009.

[2] Jaiswal, T. and Zhu, R. Software Requirements Specification for Larkut.com [Online]. 2010. Available from : http://www.docstoc.com/docs/70626850/SocialNetwork Websitedocx---Software-Requirements-Specification [2013,April 23]

[3] สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์. รายงานวิจัยฉบับสมบูรณ์การคุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในบัตรประจาตัวประชาชนแบบอเนกประสงค์ (Smart Card) [Online]. 2549. Available from : http://www.cabinet.thaigov.go.th/acrobat/smart%20card.pdf [23 เมษายน 2556]

[4] Wikipedia. Privacy [Online]. 2011. Available from : http://en.wikipedia.org/wiki/Privacy [2013,April 23]

[5] E. Kavakli, C. Kalloniatis, and S. Gritzalis Addressing privacy: matching user requirements to implementation techniques. Hellenic European Research on Computer Mathematics & its Applications Conference, 2005

[6] Wang Yang. Privacy-Enhancing Technologies. Handbook of Research on Social and Organizational Liabilities in Information Security. pp.203-227. IGI Global, 2009.

[7] OECD. About the OECD [Online]. 2010. Available from : http://www.oecd.org/about/ [2013,April 23]

[8] OECD. Privacy and Personal Data Protection [Online]. 2007. Available from : http://www.oecd.org/sti/interneteconomy/37626097.pdf [2013,April 23]

[9] RTGS. Notification on the Electronic Transactions Commission on Policy and practice Statement on Personal Data Protection of a Government Agency 2010 [Online]. 2010. Available from : http://www.ratchakitcha.soc.go.th/DATA/PDF/2553/E/126/31.PDF [2013,April 23]

[10] TRUSTe. Privacy Program Requirements [Online]. 2012. Available from : http://www.truste.com/privacy-program-requirements [2013,April 23]

[11] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ศูนยเทคโนโลยีอิเล็กทรอนิกสและคอมพิวเตอรแหงชาติ. Privacy Policay & Trustmark. 2548. Available from : http://www.nectec.or.th/pub/books/privacy-policy.pdf [23 เมษายน 2556]

[12] Wikipedia. Privacy-enhancing technologies [Online]. 2007. Available from : http://en.wikipedia.org/wiki/Privacy-enhancing_technologies [2013,April 23]

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

[14] Bouguettaya, A.R.A. and Eltoweissy, M.Y. Privacy on the Web: facts, challenges, and solutions. IEEE Security & Privacy Vol.1 No.6 (December 2003): 40-49.

[15] Deng, M., Wuyts, K., Scandariato, R., Preneel, B., and Joosen, W. A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requirements Engineering Vol.16 No.1 (2011):3-32.

[16] Al-hamdi, O., and Salah, A. Open Source Web Content Management Systems to Build Social Network Websites. International Journal of Reviews in Computing Vol.11 (September 2012): 48-60.

[17] Curry, R., Kiddle, C., Simmonds, R., and Pastorello, G.Z. An on-line collaborative data management system. Gateway Computing Environments Workshop (Nov 2010): 1-10.

[18] CAPTERRA. Alumni Management Software Programs [Online]. 2011. Available from : http://www.capterra.com/alumni-management-software [2012, October 10].

[19] Wikipedia. Web content [Online]. 2013. Available from : http://en.wikipedia.org/wiki/Web_content [2013,April 23]

[20] The IT Law Wiki. Personal Data [Online]. 2012. Available from : http://itlaw.wikia.com/wiki/Personal_data [2013,April 23]

[21] The IT Law Wiki. Personally identifiable information [Online]. 2012. Available from : http://itlaw.wikia.com/wiki/Personally_identifiable_information [2013,April 23]

[22] Wikipedia. Personally identifiable information [Online]. 2012. Available from : http://en.wikipedia.org/wiki/Personal_information [2013,April 23]

[23] UT Health Science Center. Do you know the difference between Privacy and Confidential? [Online]. 2009. Available from : http://research.uthscsa.edu/ocr/Privacy%20and%20Confidentiality%20in%20Human%20Research.pdf [2013,April 23]

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

[25] Bevanda, V., Azemovic, J., and Music, D. Privacy Preserving in eLearning Environment (Case of Modeling Hippocratic Database Structure). 4th Balkan Conf. in Informatics, pp.47-52. September 2009.

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

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

[28] Intel. Privacy Requirements and Recommendations for Application Development for the Intel AppUp developer program: What Application Developers Should Know [Online]. 2011. Available from : http://software.intel.com/en-us/articles/privacy-requirements-and-recommendations-for-application-development-for-the-intel-appupsm [2013, April 23]

[29] Romanosky, S., Acquisti, A., Hong, J., Cranor, L.F., and Friedman, B. Privacy patterns for online interactions. The conf. on Pattern languages of programs, USA: ACM, 2006.

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

[31] Costello, C. Elgg 1.8 Social Networking, 2sd ed. Birmingham: Packt Publishing, Febuary, 2012.

[32] Elgg. Welcome to Elgg's plugin directory [Online]. 2012. Available from : http://community.elgg.org/plugins [2013,January 26]

[33] Wikipedia. Comparison of social networking software [Online]. 2012. Available from : http://en.wikipedia.org/wiki/Comparison_of_social_networking_software [2013, January 26]

[34] Fory, D. Social Network / Community / Forum Software Comparison Chart [Online]. 2009. Available from : http://www.deanflory.com/articles/social_software_comparison [2013,January 26]

[35] Sharma, M. Users, Profiles, and Connections in Elgg [Online]. 2008. Available from : http://www.packtpub.com/article/users-profiles-and-connections-in-elgg [2013, January 26]

[36] Facebook. Making Your Settings Easier to Find: Dig Into the Details [Online]. 2012. Available from: https://www.facebook.com/about/details [2013, April 23]

[37] AppleInsider. US congressmen inquire about iOS privacy with Apple, 33 developers [Online]. 2012. Available from: http://appleinsider.com/articles/12/03/22/us_congressmen_ inquire_about_ios_privacy_with_apple_33_developers [2013,Febuary 25]

ประวัติผู้เขียนวิทยานิพนธ์

นายกิตติศักดิ์ สะอาดเอี่ยม เกิดเมื่อวันที่ 9 สิงหาคม พ.ศ. 2525 ที่จังหวัดสุรินทร์ เป็นบุตรชายคนแรก ของพันตรีบุญส่ง และนางมาลี สะอาดเอี่ยม สำเร็จการศึกษาระดับปริญญาวิศวกรรมศาสตร์บัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์ จากมหาวิทยาลัยเกษตรศาสตร์ วิทยาเขต ศรีราชา ในปี พ.ศ. 2548 และได้เข้าศึกษาต่อในระดับปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในภาคการศึกษาต้น ปีการศึกษา 2552