PRIVACY BY DESIGN
FOR
SOCIAL NETWORKS

Presenter: Mohammad Badiul Islam
Principal Supervisor: Dr. Jason Watson
Associate Supervisor: Adpro Dr. Renato Iannella
Associate Supervisor: Aspro Dr. Shlomo Geva
Outline

Background

Literature Review

Research Methodology

User Centered Privacy Framework (UCPF)

Privacy protecting principles

SN user privacy requirements

User Centered Privacy Architecture (UCPA)
Millions of users are connected. Facebook has roughly more than 700 million users\(^1\), Twitter roughly over 175 million registered users\(^2\); LinkedIn roughly over 100 million users\(^1\)

72% of online adults are social networking site users\(^3\)

---


\(^3\) [http://apo.org.au/research/72-online-adults-are-social-networking-site-users](http://apo.org.au/research/72-online-adults-are-social-networking-site-users)
Background

- The initial obligation was to be connected, share personal information & online activities using virtual spaces in Social Networks (SN).
- Technical breaches in SN become a source of identity theft, unauthorized access, illegal use of information (Patil & Kobsa, 2009).
- Users and consumers are beginning to show anxiety for privacy in SN (Cavoukian, 2009).
- User and specialists are looking at the privacy impact of such large-scale sharing.
- 90% of the 5,627 respondents in 22 countries ranked privacy as troubling issue (KPMG International Cooperative, 2010).
- Privacy may not exist by the year 2020 (Cavoukian, 2010a).
- Every person has the right to share, disclose, access, rectify, delete, and block their own personal information unless there are legitimate reasons provided by law (European Commission, 2010).
- There is a conflict between SN objectives, and privacy protection. By definition, SNs promote sharing through SN functionalities.
- Privacy does not mean simply hiding information; it is the legitimate control over one’s own personal information.
- Researchers identifying that “something” needs to be done since private information may be stored forever in public places (Langheinrich, 2001).
Practical Significance

- SNs providers do not necessarily guarantee privacy and security of the members. For examples, Facebook Privacy policy\(^1\) states that:

  “We cannot control the actions of other users with whom you share your information. We cannot guarantee that only authorized persons will view your information. We cannot ensure that information you share on Facebook will not become publicly available. We are not responsible for third party circumvention of any privacy settings or security measures on Facebook.”\(^1\)

- SN may be free, but we give up our precious information. That’s the price we pay to be social\(^2\).

- There is no such thing as privacy on SN since at the end, we’re agreeing to sign up to use a SN service and agree to what they say\(^2\).

\(^1\)http://www.facebook.com/policy.php
\(^2\)http://theantisocialmedia.com/tag/cartoon/page/7/
Practical Significance

Google continues social-networking push with Angstro buy
By Scott Collins
August 17, 2010 3:50 AM EDT

IDO News Service - Google continues to aggressively pursue social-networking capabilities, this time with the acquisition of Angstro.

Angstro is a small organization with a few products including Noteworthy.

Teenager arrested for Facebook post beaten up in prison
RT - 03/07/2013
Things aren't getting any better for a 19-year-old video gamer who has been locked up since March for the remarks he made on Facebook.

Show less

Weekly Wrapup: Facebook Buys FriendFeed, Distributed Social Networking, Google Caffeine, And More...

By ReadWriteWeb
In this edition of the Weekly Wrapup, our newsletter comes directly from the recent Wrapup post on the ReadWriteWeb blog.

We are taking a look at this week's biggest news in the space. This week, we see that Facebook is back in the game with the acquisition of FriendFeed, while Google has launched a search product called Caffeine.

Facebook could cost you your job!
Emma Roberts

Emma Roberts investigates how using social networking websites could be putting your career at risk.

Salesforce.com Readies Native Mobile Chatter Apps
By Colm Kavanagh, IDG News

Salesforce.com is working on a suite of native mobile applications for its Chatter collaboration platform. The company announced Wednesday Support mobile platforms include Apples iPhone, iPad and iPod Touch, Google Android and Research in Motion Blackberry.

Facebook's Like Button Total! Not Just Likes
M@Facebook 17/07/2013
Current Facebook developers' documentation doesn't confirm this. And if your visitor's friends like or comment on your visitor's share story ...

Home > News
Police: Girl missing from Needham claimed she was heading to party in Lynn
By Robin Kaminski / The Daily Item
LYNN - Police are asking for the public's help in locating a missing Needham teen who came to Lynn Saturday night in search of a party and never returned.

Lynn party and fees she may have sent a boy on Facebook and then arranged to meet him. The last time Anyone spoke with her family was around 11 p.m.

Victim of hatchet job on Facebook
Times LIVE - 5 hours ago
Victim of hatchet job on Facebook: Power-obsessed leaders fiddle ...
Victim of hatchet job on Facebook Victim of hatchet job on Facebook

I recognise myself in natty 'Rhodes confessions'. I know who writes these lies. What do I do?
Practical Significance

Different privacy rights and requirements
Research Significance

- The privacy problem is complex and users want privacy but they seldom know “how to specify” and “what to seek” for their own privacy (Shapiro, 2009).

- SN service providers offer different services and functions such as edit, share, export, delete SN data type, often, it is not clear what rights (Schneier, 2010) or privacy requirements SN users really have.

- SN privacy requirements must not be ad-hoc or post-fact (Cavoukian, 2009).

- Ensure privacy from the beginning of a system development (Cavoukian, 2009) (Langheinrich, 2001).
  
  - Embedded privacy-enhancing technologies at the design level?

- SN service provider may use different principles to protect user information.
  
  - Which principles are the best to ensure privacy protection in SN from design level?

- There are neither mechanisms nor processes on
  
  - How to convert privacy protecting principles across Social Networks.
  
  - How these principles must be built into the way information is protected
  
  - Must be supported by SN functionalities and practices.
Research Questions

How can user privacy be protected within Social Networks?

i. What are the privacy requirements of Social Networks users?

ii. What are the principles required to protect user privacy in Social Networks?

iii. How effective are the privacy principles employed by the Social Networks providers? How can these be converted to a usable framework?

iv. How does the privacy framework inform Social Networks architecture?
Literature Review

- What is Social Network?
- What is privacy?
- Why should we care about Social Networks?
- User information and privacy in Social Networks
- Behind Privacy in Social Network
- Location based privacy
- Privacy in Mobile Social Network Services

Social Network and privacy

Privacy Protection Mechanism

Architecture Models and methodologies

Privacy protecting architectures

- Enterprise perspective
- Privacy by Innovative Architecture
- Privacy by design
- Individual users perspective
- Privacy by Access Control
- Privacy by Friends-of-a-friend prediction

- Client-server architecture
- Distributed architecture
- Third party architecture
- Peer-to-peer or ubiquitous architecture
- Wireless sensor networks architecture
- Open source architectures

- Access Control model
- Minimal information sharing
- Third party model
- The Zachman Framework for Enterprise Architectures
- The Open Group Architectural Framework (TOGAF)
- The Federal Enterprise Architecture
- The Gartner Methodology
Literature Review

What is privacy?

Westin (2003) empirically derived three privacy positions that public holds.
Literature Review

SN user data types

- SN, services deal with different data types (private, protected and public) (Hart & Johnson, 2010).

- Six types of SN user data (Schneier, 2010), (Madejski, et al., 2011)
## Literature Review

<table>
<thead>
<tr>
<th>Architectural models</th>
<th>Minimal information sharing</th>
<th>Third party model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control model</td>
<td>Cryptographic techniques such as join and intersection operations to secure information.</td>
<td>Engages a untrusted third party or Trusty third party (C. Y. Chow, 2010)</td>
</tr>
<tr>
<td></td>
<td>De-identification and “re-identification information” (Narayanan &amp; Shmatikov, 2010)</td>
<td>Practical examples: <strong>Anonymizer</strong> for anonymous web surfing <strong>PayPal</strong> for buying/selling products</td>
</tr>
<tr>
<td></td>
<td>Computational cost and inability to facilitate other queries make this paradigm unsuitable for real time applications (C. Y. Chow, 2010)</td>
<td>Computational cost and emphasis on processing securing information from multiple data sources make this paradigm unsuitable for real time applications (C. Y. Chow, 2010)</td>
</tr>
</tbody>
</table>

Have little choice to focus on how data is used and how data is accessed by different stakeholders (Kagal & Abelson, 2010)
Architecture Methodologies

- The Zachman Framework for Enterprise Architectures
- The Federal Enterprise Architecture
- The Gartner Methodology
- The Open Group Architectural Framework (TOGAF)
  - TOGAF Scores better

  - Process completeness
  - Vendor neutrality
  - Information availability as necessary to promote sharing and disclosure for SN users (Wallbridge, 2009), (Spiekermann & Cranor, 2009), (Tan, et al., 2012)

- TOGAF enables frameworks to be tailor made
- TOGAF offers Boundary less Information Flow
- TOGAF offers open systems implementation.

Research gaps and motivations

- Most of the SN have limited options for customizing the privacy preferences (Rosen, 2010)

- Required to consider technical, non technical, legislative, judicial, and ethical issues to protect and share user information in SNs (Davies, 2010) (Le Métayer, 2010)

- As quick solution
  - Clustering privacy preferences (Cai, Wang, Gong, Chen, & Ma, 2009) (Sören Preibusch, 2008)
  - Setting up canonical policies (Rosen, 2010)
  - access control mechanism (G Lugano & P Saariluoma, 2009)

- As long term solution (Privacy Rights Clearinghouse, 2011)
  - Raising awareness
  - Involve legislative bodies
  - Offer several technical solution

- As permanent solution
  - Privacy by Design can be adapted into Social Networks design level (Cavoukian, 2009)
### Research Methodology

**Integration of case study and survey methods** *(Gable, 1994)*

<table>
<thead>
<tr>
<th>Investigation</th>
<th>Research Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Construct SN users Privacy requirements.</td>
<td>Mix methods (Quantitative &amp; Qualitative analysis)</td>
</tr>
<tr>
<td></td>
<td>Survey</td>
</tr>
<tr>
<td>Represent the principles required to protect SN user privacy.</td>
<td>Literature Review</td>
</tr>
<tr>
<td></td>
<td>Case Study</td>
</tr>
<tr>
<td>Evaluate the effectiveness of these principles employed by the SN providers.</td>
<td>Case Study</td>
</tr>
<tr>
<td>Represent these principles into a usable framework.</td>
<td>TOGAF©</td>
</tr>
<tr>
<td>Design SN architecture based on the privacy framework.</td>
<td>TOGAF©</td>
</tr>
</tbody>
</table>
Investigating SN user privacy requirements

- Review and synthesize SN user privacy requirements
- Six stages of Thematic analysis method as analytical framework (Braun & Clarke, 2006)

10 Primary and 42 Secondary SN user privacy requirements

Pre-pilot assessment
- Assess SN user privacy requirements by a panel of expert judges

5 Primary and 32 Secondary SN user privacy requirements

Pilot survey
- Assess by experts in privacy and social Network areas
- Descriptive analysis

Survey (Open & closed ended questions)
- Validated by general SN users through a Quantitative analysis using IBM SPSS Statistics 21 and IBM SPSS Amos 21
- Explore new factors through Qualitative analysis

5 Primary and 25 Secondary SN user privacy requirements
## Findings: SN user privacy requirements

<table>
<thead>
<tr>
<th>Primary privacy requirements</th>
<th>Secondary privacy requirements</th>
<th>Analysis code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Control</td>
<td>Information addition</td>
<td>IC1</td>
</tr>
<tr>
<td></td>
<td>Information deletion</td>
<td>IC2</td>
</tr>
<tr>
<td></td>
<td>Information sharing</td>
<td>IC3</td>
</tr>
<tr>
<td></td>
<td>Information altering</td>
<td>IC4</td>
</tr>
<tr>
<td></td>
<td>Information re-uses</td>
<td>IC5</td>
</tr>
<tr>
<td></td>
<td>Information export</td>
<td>IC6</td>
</tr>
<tr>
<td></td>
<td>Control over fixing privacy issues even not the member of SN</td>
<td>IC7</td>
</tr>
<tr>
<td>Information collection and storage</td>
<td>Information collection and storage</td>
<td>CS1</td>
</tr>
<tr>
<td></td>
<td>Analysis of collected and stored information</td>
<td>CS2</td>
</tr>
<tr>
<td></td>
<td>Notification for information collection and storage</td>
<td>CS3</td>
</tr>
<tr>
<td></td>
<td>Disposal of collected and stored information</td>
<td>CS4</td>
</tr>
<tr>
<td>Information access</td>
<td>Information access</td>
<td>IA1</td>
</tr>
<tr>
<td></td>
<td>Communication</td>
<td>IA2</td>
</tr>
<tr>
<td></td>
<td>Information access by copying</td>
<td>IA3</td>
</tr>
<tr>
<td></td>
<td>Information access by using mobile or hand held devices</td>
<td>IA4</td>
</tr>
<tr>
<td></td>
<td>Information access by tracking</td>
<td>IA5</td>
</tr>
<tr>
<td></td>
<td>Behavioral information access</td>
<td>IA6</td>
</tr>
<tr>
<td>Unauthorized secondary use (Internal &amp; External)</td>
<td>Secondary information uses</td>
<td>UU1</td>
</tr>
<tr>
<td></td>
<td>Location information uses</td>
<td>UU2</td>
</tr>
<tr>
<td></td>
<td>Implicit secondary information uses</td>
<td>UU3</td>
</tr>
<tr>
<td>SN Practice</td>
<td>Information disclosure</td>
<td>SP1</td>
</tr>
<tr>
<td></td>
<td>Notification of linking information e.g. location information, behavioral information with content</td>
<td>SP2</td>
</tr>
<tr>
<td></td>
<td>Practice accountability</td>
<td>SP3</td>
</tr>
<tr>
<td></td>
<td>Practice visibility and transparency e.g. How see a particular content</td>
<td>SP4</td>
</tr>
<tr>
<td></td>
<td>Notification for any type of information changes</td>
<td>SP5</td>
</tr>
</tbody>
</table>

SN user privacy requirements are classified & represented as SN practices and control of that practices.
Investigating privacy protecting principles

- Reviewed existing privacy protecting principles
- Identified privacy protecting principles for SN to ensure PET
- Privacy by Design (PbD)
  - Investigate PbD approaches in privacy invasive areas
  - Design two cases studies: Diaspora & Clique
  - Assess on how SN follow the PbD principles
  - Map users privacy requirements with PbD principles
Findings for Privacy protecting principles

<table>
<thead>
<tr>
<th>Privacy by Design (PbD) principles</th>
<th>Can be used for adopting PET directly at the SN system design level (Cavoukian, 2009).</th>
</tr>
</thead>
<tbody>
<tr>
<td>(7 Principles)</td>
<td>Will increase the use of PET and FIP SN (Blarkom, et al., 2003)</td>
</tr>
<tr>
<td>Proactive not Reactive; Preventative not Remedial</td>
<td>Can be used to ensure SN practices and control of that practices (Cavoukian, 2009). (Raab, 2004)</td>
</tr>
<tr>
<td>Privacy as the Default</td>
<td>Implement nine attention areas for compliance auditing (Blarkom, et al., 2003):</td>
</tr>
<tr>
<td>Privacy Embedded into Design</td>
<td>i) Intention and notification</td>
</tr>
<tr>
<td></td>
<td>ii) Transparency</td>
</tr>
<tr>
<td></td>
<td>iii) Finality principle</td>
</tr>
<tr>
<td></td>
<td>iv) Legitimate grounds of processing</td>
</tr>
<tr>
<td></td>
<td>v) Quality</td>
</tr>
<tr>
<td></td>
<td>vi) Data subject’s rights</td>
</tr>
<tr>
<td></td>
<td>vii) Security</td>
</tr>
<tr>
<td></td>
<td>viii) Processing by a processor</td>
</tr>
<tr>
<td></td>
<td>ix) Transfer of personal data outside the network</td>
</tr>
<tr>
<td>Full Functionality – Positive-Sum, not Zero-Sum</td>
<td></td>
</tr>
<tr>
<td>End-to-end Security- Full Lifecycle Protection</td>
<td></td>
</tr>
<tr>
<td>Visibility and Transparency- Keep it open</td>
<td></td>
</tr>
<tr>
<td>Respect for User Privacy</td>
<td></td>
</tr>
</tbody>
</table>
Findings: Two case studies

- For two open source SN Diaspora and Clique (claimed privacy-aware SN)
- A set of “Assessment Criteria” was formulated according each PbD principles.
- Produce “Privacy Score” for Diaspora and Clique system features
  (0-‘None’, 1–‘Low’, 2 –‘Medium’ & 3 –‘High’ comply)

- Overall, Diaspora and Clique followed only some of the PbD principles
- Consequently failed to ensure full privacy
- Diaspora substantiated securing personal content whereas
- Clique focused to solve privacy issues from SN user perspective

![Bar chart showing privacy scores for Diaspora and Clique]
Business and technology strategy

Three way mapping was established as a technology and business architecture strategy to enhance privacy at the design level of the privacy framework.
Findings: User Centered Privacy Framework (UCPF)

The freely available “The Open Group Architecture Framework (TOGAF®)”\textsuperscript{1,2} was used to develop the “step by step” framework and architecture.

\textsuperscript{1} http://www.opengroup.org/togaf/
\textsuperscript{2} http://pubs.opengroup.org/architecture/togaf9-doc/arch/
Preliminary stages & Architecture vision

Architectural method, principles, vision and requirement

- Preliminary: method and principles
- Architecture vision
  - Stakeholders
  - Business and technology strategy
- Architectural Requirements

SN Stakeholders and actors

Legend
- Private information
- Protected information
- Public information
Stage B - Business architecture

Business architecture

Organization unit

Driver

Goal

Objective

Measure

Motivation

Actor

Function

Role

Process

Business services

Data Entity

Logical Data Component

Logical Technology Component

Platform service

Data architecture

Technology architecture
Information Flow through process and functions
Stage C-Data Architecture

Data architecture

SN Data types and entities

- Service data
  - Basic profile information
  - Legal name
  - Credit-card number

- Disclosed data
  - Basic profile information
  - Basic page memberships
  - Photographs information
  - Comments on photographs
  - Album information
  - Comments on albums
  - Links
  - Comments on links
  - Status updates
  - Comments on status updates
  - Wall posts
  - Comments on wall posts
  - Notes
  - Comments on notes
  - Video information
  - Comments on videos
  - Behavioral data
    - Games user plays
    - News articles that user access
    - Topics user write about
    - User activities
    - User does any activities with whom
    - What user says about political learnings

- Entrusted data
  - Comments on friend's albums
  - Comments on friend's notes
  - Comments on friend's tagged notes
  - Comments on friend's photos
  - Comments on friend's tagged photos
  - Comments on friend's status updates the participant was tagged in
  - Comments on friend's videos
  - Comments on friend's tagged videos
  - Comments on friend's wall
  - Event RSVPs
  - Public group memberships

- Incidental data
  - Comments on friend's status updates the participant was tagged in
  - Comments on participant's albums
  - Comments on participant's links
  - Comments on participant's notes
  - Comments on participant's tagged notes
  - Comments on participant's videos
  - Comments on participant's wall
  - Comments on status updates
  - Comments on the participant's photos
  - Status updates the participant was tagged in

- Derived data
  - Derived data from any other data types

Network awareness

- Disclosed data
- Entrusted data
- Incidental data

Expert search

- Service data
- Disclosed data
- Entrusted data
- Incidental data
- Behavioral data
- Derived data

Context awareness

- Service data
- Disclosed data
- Entrusted data
- Incidental data
- Behavioral data
- Derived data

Contact Management

- Service data
- Disclosed data
- Entrusted data
- Incidental data
User Centred Privacy Model (UCPM)
User Centred Privacy Model (UCPM)

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Service provider</th>
<th>Third parties</th>
<th>External parties</th>
</tr>
</thead>
<tbody>
<tr>
<td>A friend</td>
<td>A friend of a friend</td>
<td>A network member</td>
<td>A friend of a friend</td>
</tr>
</tbody>
</table>

SN User privacy requirements: IC: Information Control, CS: Information collection and storage, IA: Information access, UU: Unauthorized secondary use (Internal & External), SP: SN Practice

Data types (IC 1, IC 2, IC 3, IC 4, IC 5, IC 6, CS 1, CS 2, CS 3, CS 4, IA 1, IA 2, IA 3, IA 4, IA 5, IA 6, UU 1, UU 2, UU 3, SP 1, SP 2, SP 3, SP 4, SP 5)

HP (High Privacy)  BP (Balanced Privacy)  LP (Low Privacy)

NICTA Copyright 2010 From imagination to impact
Message Sequence of Privacy model
Use case

Lets imagine- “Alice participated in a political demonstration and uploaded her photos and activities onto her Social Network. She has set the default privacy to “balanced”.

She wants to set “High” privacy for her new photos so that only one predefined “Political Group of friends” can see them and they cannot reuse these photos”.

- Two groups: “Political group of friends” and Other Stakeholders
- Alice has “balanced” so, she is apathetic for her privacy requirements and data types. She wants to set “High” privacy for her uploaded photo and deny to reuse political “Group of friends”.
- Uploaded photo’s data type is “Disclosed data” and analysis code is “DD3”.
- Alice sets “HP” for DD3 for IC5- Information re-uses & “LP” for each of the SN user privacy requirements for “Political group of friends”
- Alice sets “HP” for DD3 for each of SN privacy requirements for Other Stakeholders.
Setting up the UCPM for the use case

SN stakeholders access user data based on privacy positions and privacy requirements.
# Use case

## Stakeholders

<table>
<thead>
<tr>
<th>Users</th>
<th>Political group</th>
</tr>
</thead>
</table>

## SN User privacy requirements:
- **IC**: Information Control
- **CS**: Information collection and storage
- **IA**: Information access
- **UU**: Unauthorized secondary use (Internal & External)
- **SP**: SN Practice

### Data types

| IC1 | IC2 | IC3 | IC4 | IC5 | IC6 | IC7 | CS1 | CS2 | CS3 | CS4 | IA1 | IA2 | IA3 | IA4 | IA5 | IA6 | UU1 | UU2 | UU3 | SP1 | SP2 | SP3 | SP4 | SP5 |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| HP (High Privacy) | BP (Balanced Privacy) | LP (Low Privacy) |

---

## Stakeholders

<table>
<thead>
<tr>
<th>Users</th>
<th>Service provider</th>
<th>Third parties</th>
<th>External parties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other friends or groups</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## SN User privacy requirements:
- **IC**: Information Control
- **CS**: Information collection and storage
- **IA**: Information access
- **UU**: Unauthorized secondary use (Internal & External)
- **SP**: SN Practice

### Data types

| IC1 | IC2 | IC3 | IC4 | IC5 | IC6 | IC7 | CS1 | CS2 | CS3 | CS4 | IA1 | IA2 | IA3 | IA4 | IA5 | IA6 | UU1 | UU2 | UU3 | SP1 | SP2 | SP3 | SP4 | SP5 |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| HP (High Privacy) | BP (Balanced Privacy) | LP (Low Privacy) |
Verification of the privacy model

Use UPPAAL Model to simulate, check the Privacy model and focused on process paths

- There was no deadlock.
- There was a reachable state in which user is able to define their privacy position.
- There was a reachable state in which user is able to define their privacy requirements.
- There was a reachable state in which user is able to define their stakeholders.
- There was a reachable state in which user is able to complete upload data by protecting privacy from stakeholders.
- There was a reachable state in which stakeholder is able to access user information by protecting privacy.
Conclusion

What are the privacy requirements of Social Networks users?

- Proposed a new set of SN user privacy requirements and constructed five (5) primary user requirements and Twenty Five (25) Secondary
- Potential to *SN users* to provide more sophisticated privacy controls and essential rights and requirements and what they want to do with their own SN data
- Potential for *SN service providers* to better design and improves the old or implements a new SN service using an enhanced understanding of essential *SN user* rights and privacy requirements
- Potential for *SN stakeholders* for greater understanding of *Privacy in SN* context through the new concept of *privacy*.
- *Privacy* is classified and represented as *SN practices* and control of these practices in SN.
Conclusion

What are the principles required to protect user privacy in Social Networks?

- Presents seven existing leading privacy protection principles and determines which principles are the best instruments to ensure privacy protection in SN.

- *SN service providers* now have a set of privacy protecting principles to protect Personally Identifiable Information (PII) of SN users and facilitate privacy-enhancing technologies (PETs) from earliest design stage SN.

- *SN service providers* are able to ensure Fair Information Principles (FIPs) and implement nine attention areas for compliance auditing.
Conclusion

How effective are the privacy principles employed by the Social Networks providers? How can these be converted to a usable framework?

- Evaluated the effectiveness of PbD principles by assessing on how real world SN test cases perform.
- None of the test cases fully comply with PbD principles and consequently failed to ensure full privacy.
- Established new knowledge in engaging PbD principles in SN.
- Established a new formal and conceptual privacy framework *User Centred Privacy Framework (UCPF)* engaging PbD principles
Conclusion

How does the privacy framework inform Social Networks architecture?

- Presents a three level *User Centred Privacy Architecture (UCPA)*: Business, Data, technology architecture for *SN service providers* to incorporate privacy at the design level.

- A new privacy model, *User Centred Privacy Model (UCPM)* enables *SN users* to specify their rights and privacy requirements.

- Designed and developed *UCPF* and *UCPA* using TOGAF®

- Created *UCPF, UCPA and UCPM* to achieved the goal of a more accurate, effective and efficient user centred SN.
Limitation and future work

- Focused only on the technical dimensions and did not consider legal and social dimensions of privacy.

- Future research can be extended by harmonizing the understanding between regulators, engineers, business managers and politicians since accepting PbD principles may be a political choice.

- A greater number of survey participants may increase the acceptance of the findings.

- Did not consider traditional and closed source or enterprise SN Yammer\(^1\) to evaluate PbD principles.

- Did not develop conceptual application architecture level for UCPA or implement a Social Network service based on UCPF and UCPM.

- Large scale testing was not undertaken and UCPF, UCPA and UCPM were not validated globally on well-known SN such as Facebook, LinkedIn and Twitter.

\(^1\)http://www.yammer.com/
Publications arising from this thesis

Published

Refereed Book Chapter


Refereed workshop paper


Papers under review

Privacy in Social Networks: a survey of state-of-the-art
What I want for my Social Network privacy?
User Centred Privacy Model (UCPM): Bring your own privacy model for Social Network
Questions?

Thank you