USER-CENTRIC PRIVACY PRESERVATION IN SOCIAL NETWORKS

Amir H. Chinaei, Rosa Karimi Adl, Chenen Liang, Ken Barker
University of Calgary, University of Waterloo
Canada

EMCIS 2009, Izmir Turkey

AGENDA

- Introduction
  - Motivations behind Social Network usage
  - Sample study on information revelation
- Risks in Online Social Networks (OSN)
  - Stalking
  - Building a digital dossier
  - Re-identification
  - Fragile privacy protection
- Call for user centric privacy mechanism
- Adoption of User-Centric Privacy Preservation Method
- Conclusion
INTRODUCTION

Motivations behind Social Network usage:
34 million (67%) of Americans age 18-29 use OSNs [The Pew Research Center For The People And The Press Jan 11, 2008]

Why?
- Meeting new people
- Finding new jobs
- Keeping in touch with friends in other places
- Receiving and/or providing recommendations
- Keeping informed about social events in a group

Sample study on information revelation:
Based on a study on network of Carnegie Mellon University: (Gross, Acquisti, & Heinz, 2005)
INTRODUCTION (CONT.)

Why individuals provide large amount of information?

- Only small portions of users tend to change the default privacy preferences.
- People are not concerned about their privacy.
- Users intentionally publish their personal information publicly. (signaling)

ONLINE VS. OFFLINE SOCIAL NETWORKS

<table>
<thead>
<tr>
<th>Online Social Networks</th>
<th>Offline Social Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binary Relations:</td>
<td></td>
</tr>
<tr>
<td>• No weight for relationship</td>
<td>Notions of weak and strong ties</td>
</tr>
<tr>
<td>• Friend or Not</td>
<td></td>
</tr>
<tr>
<td>Cheap and easy way of adding weak ties</td>
<td>Network expansion is not easy</td>
</tr>
<tr>
<td>Network is vaster and have more weak</td>
<td>Network is not vast</td>
</tr>
<tr>
<td>ties</td>
<td></td>
</tr>
</tbody>
</table>

There might be less trust within an online social network.
RISKS IN OSNs

Stalking:

- Residence Location + Class schedule + Location of last login
  \[\rightarrow\]
  likely physical location of user

- AOL Instant Messenger \[\rightarrow\] Is the user online or offline?

Building a digital dossier:

- Unimportant private information may become important in future

RISKS IN OSNs (Cont.)

Re-identification:

- Demographics Re-identification
  - user’s profile JOIN his records in other databases

- Face re-identification:
  - face recognition tools \[\rightarrow\] matches between two profiles in different social networking sites

- SSN and identity theft:
  - • Hometown
  - • Date of birth
  - • Current residence
  - • Phone number \[\rightarrow\] Estimate on Social Security Number
RISKS IN OSNs (Cont.)

Fragile privacy protection:

- Protection mechanism can be circumvented
- Users have little control on the composition of their network
- Manipulating (corrupting) users
- The number of needed manipulated users decreases exponentially as the lookahead increases. (Korolova, Motwani, Nabar & Xu, 2008)
- Ask to be added as someone’s friend: 30% of people accept!

CALL FOR USER CENTRIC PRIVACY MECHANISM

Privacy rules in social networking:
(Bruce Schneier, 2006)

The rules call for some user centric privacy protection mechanism

People are willing to share all sorts of information as long as they are in control.
People believe that they own their data even though the user agreement might technically give companies the right to sell the data.

Adopt User-Centric Privacy Preservation Method
ADOPTION OF USER-CENTRIC PRIVACY PRESERVATION METHOD

The Universe:

- Objects
  - Passive
  - Semi-Public
  - Private
  - All members

Identity
- name, contact information, DOB, Marital status

Semi-Public
- category based user interests, current/previous school and employer, user’s wall, communities and groups, friends

Private
- religious views, political views, sexual preferences, drinking and drug habits

Access Authorization:

Access constraint:
- Visibility (V)
- Generalization (n)
- Purpose (P)
- UDC

Visibility (coarse grained):

Visibility Axis
- Friends
- Friends of a friend
- Stranger
ADOPTION OF USER-CENTRIC PRIVACY PRESERVATION METHOD (Cont.)

Visibility (fine grained):

- **Visibility Axis**
  - Friends
  - Friends of a friend
  - Stranger
  - Arbitrary hierarchy
  - groups based on the distance in the underlying graph

- **Automatic tool for one level categorization**:
  (AduOppong, Gardiner, Kapadia, & Tsang, 2008)

- Each member of a specific sub-graph should have:
  - at least $\beta$ friends in his own sub-graph
  - at most $\alpha$ friends in other sub-graphs.

---

Generality (n): Depends on the type of object:

- **Name:** Rosa Karimi, R. Karimi, Rosa K., R. K., Rosa, Karimi
- **Numerical values:**
  - dropping some digits, or
  - expressing them in a range
- **Photo:** adding some noise and decreasing quality

Purpose (p): Read and update

UDC: Those that are concerned with time and location

- **Example:** Time constraints on availability of user's wall
ADOPTION OF USER-CENTRIC PRIVACY PRESERVATION METHOD (Cont.)

Access Banks:

- Owner bank is created as soon as a piece of information is uploaded
- User can define customized banks

Example Uploading a photo:
- Owner is the one who uploads the photo
- Owner defines (fertile) customized banks for other people in the photo
- Members of the customized bank can:
  - restrict visibility,
  - increase generality,
  - restrict purposes or
  - add more UDC.

And make new customized bank.

CONCLUSION

- Decreased trust in online social networks
- Several Potential Privacy risks in Online social networks
- Unconcerned users to privacy risks
- Social Networks call for serious privacy considerations
- A seemingly feasible solution is adopting the User-Centric Privacy Preservation Method
REFERENCES


Thank you