463.2 Social Networks

Computer Security II
CS463/ECE424
University of Illinois
Under which of those categories do you think privacy settings belong?

“renamed them to more closely match people’s mental models,” so it should be obvious. Just use your mental model.

If your answer is “all of them, conceivably,” congratulations, you got it! Now if you want to update your privacy settings, all you need to do is visit all of these new categories and subcategories individually. Any one of them might have a crucial toggle inside — it’s like a treasure hunt!

Security News of the Day
Security News of the Day

Oh, Facebook changed its privacy settings again

Devin Coldewey @techcrunch / 6:33 PM CDT • August 4, 2021

We joke, but Facebook did also make the “Privacy Checkup” item much more prominent in this update. This “guided review” may give the company opportunities to employ dark patterns that lure users away from less desirable (for the company) privacy choices, but does certainly go through many of the more important settings and let people change them.

Homophily in Social Networks
Social Network Inference
Privacy Risks
Discussion
463.2.1 Homophily in Social Networks

People of similar characteristics tend to befriend each other.
Homophily

- **Homophily** (i.e., "love of the same") is the tendency of individuals to associate and bond with similar others.
  - Term coined in 1950s in sociology papers.
- Systematically studied even earlier
- Much older concept; **Socrates to Lysis**:
  - “… and have you not also met with the treatises of philosophers who say that like must love like …”
- **Modern variant**: ‘Similarity breeds connection’
Homophily

- Shown to exist for many attributes
  - Race/Ethnicity
  - Age
  - Religion
  - Education
  - Occupation
  - Gender
  - Marriage (homogamy)

Socrates (again) speaking to a pair of youths:

*I shall not ask which is the richer of the two, I said; for you are friends, are you not?*
*Certainly, they replied.*

*And friends have all things in common, so that one of you can be no richer than the other, if you say truly that you are friends. They assented.*
Homophily: Terminology

<table>
<thead>
<tr>
<th>Choice Homophily</th>
<th>Induced Homophily</th>
</tr>
</thead>
<tbody>
<tr>
<td>Closeness due to preferences by the individual.</td>
<td>Closeness due to other constraints. Examples: Geographic closeness, Age closeness with friends.</td>
</tr>
<tr>
<td>Example: Favorite teams</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Value Homophily</th>
<th>Status Homophily</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individuals with similar values, thinking.</td>
<td>Individual with similar social status. Example: Aristocracy</td>
</tr>
<tr>
<td>Example: Religion</td>
<td></td>
</tr>
</tbody>
</table>
Geographic Homophily: Marriages

- George Zipf, studied a large number of such empirical relationships

- Is this (inverse) relationship independent of other factors?

"Human behavior and the principle of least effort" George Zipf, 1949
Geographic Homophily

• Size and distance of populations correlate with their degree of connection.

• Zipf equation:

  \[ \text{Connection} = G \times \left( \frac{\text{Pop1} \times \text{Pop2}}{\text{Distance}} \right) \]

  \( G \) is a scaling factor

Fig. 9-14. Railway express. The movement by weight (less carload lots) between 13 arbitrary cities in the U. S. A., May 1939.
Geographic Homophily: Telephone Call Graphs in Belgium
# The World's Most-Used Social Platforms

The latest global active user figures (in millions) for a selection of the world's top social media platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Active Users (in millions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>2,740</td>
</tr>
<tr>
<td>YouTube</td>
<td>2,291</td>
</tr>
<tr>
<td>WhatsApp</td>
<td>2,000</td>
</tr>
<tr>
<td>Facebook Messenger*</td>
<td>1,300</td>
</tr>
<tr>
<td>Instagram</td>
<td>1,221</td>
</tr>
<tr>
<td>Weixin / Wechat</td>
<td>1,213</td>
</tr>
<tr>
<td>TikTok</td>
<td>689</td>
</tr>
<tr>
<td>QQ</td>
<td>617</td>
</tr>
<tr>
<td>Douyin**</td>
<td>600</td>
</tr>
<tr>
<td>Sina Weibo</td>
<td>511</td>
</tr>
<tr>
<td>Telegram</td>
<td>500</td>
</tr>
<tr>
<td>Snapchat</td>
<td>498</td>
</tr>
<tr>
<td>Kuaishou</td>
<td>481</td>
</tr>
<tr>
<td>Pinterest</td>
<td>442</td>
</tr>
<tr>
<td>Reddit**</td>
<td>430</td>
</tr>
<tr>
<td>Twitter</td>
<td>353</td>
</tr>
<tr>
<td>Quora**</td>
<td>300</td>
</tr>
</tbody>
</table>

**Notes:** Platforms identified by (*) have not published updated user numbers in the past 12 months, so figures will be less reliable. (**) Figure for Douyin uses the reported daily active user figure, so monthly active user figure is likely higher.

Data updated to: 25 January 2021

---

**Sources:** We Are Social Analysis (Jan 2021), Based on data published in: (1) company statements and earnings announcements. (2) platforms' self-service ad tools.
Milgram’s Six Degrees of Separation (Small-World)

• The Six Degrees of Separation (Milgram 1967)

• Random people from Nebraska were to send a letter (via intermediaries) to a stockbroker in Boston.

• Could only send to someone with whom they were on a first-name basis.

• Not many arrived, but among the letters that found the target, the average number of links was six.
Degree of Separation on Facebook

Facebook users had 4.74 degrees of separation in 2011 (down from 5.28 in 2008, down to 3.57 in 2016)
Recent Degree of Separation for Facebook

Mean = 3.57

2016

Mark Zuckerberg
3.17 degrees of separation

Sheryl Sandberg
2.92 degrees of separation
Homophily on Facebook

- 84% of all connections are within the same country
- Ages on Facebook in 2011 show homophily
463.2.2 Attribute Inference in Social Networks
Social Networks: Inference

• It is understood by a user that the provider (e.g., Facebook) will have profile data given by the user
  – This privacy risk is ‘implicitly’ acceptable to the user

• However
  – Can the provider infer other attributes about you?
  – What can a third party infer from ‘publicly’ disclosed attributes?
Social Networks: Age Inference

- [Dey12] Estimating Age Privacy Leakage in Online Social Networks (INFOCOM 2012)
  - Used 1.4 million users in New York City (49.2 million friends)
  - Attempted to estimate age of a user
  - Had ground truth available due to Facebook’s policies in 2009, but only 1.5% of ages were public in 2010

- What attributes (other than age itself) would be most helpful for this inference?
Social Networks: Age Inference

• Use the property of age-homophily
  – Ages of friends should be similar to that of the user
  – High-school graduation year of friends should be closer to the high-school graduation of the user
  – Use information from friends of friends, etc.,

• What if the user has not made their friend list public?
Social Networks: Age Inference (Baselines)

- As a baseline, take the mean / median of the known ages in the whole dataset as the age estimate.

- The cumulative score (y-axis) shows the percentile of users whose estimate was within the error level (x-axis).
Social Networks: Age Inference

- With known high-school graduation year (HSY), age pairs
  - Train a linear-regression model for Birth Year (BY)
    - For instance, if you graduated from high-school in 1980, the birth year comes to 1963
  - If HSY is not available, use most frequent friends’ HSY (with a minimum threshold).

\[ BY = 0.9368 \times HSY + 108.2107 \]
Social Networks: Age Inference

• First Phase:
  – Known ages
  – If HSY available, estimated ages from HSY
  – If enough friends with HSY available, Estimated ages from HSY of friends

• Not all users satisfy one of the above three conditions: For those, use iterative approach
  – Estimated age of friends in the previous step
  – Iteratively do this multiple times, to gradually cover the entire graph
Social Networks: Age Inference

- Using the iterative approach, 83.8% of user ages can be identified within age error bound of 4 years.
Social Networks: Age Inference

- What if a user’s friend list is not publicly listed?
- Use reverse look up:

Fraction of hidden friend list users for whom reverse lookup can identify at least x number of friends
More sophisticated inferences

- [Mislove10] “You are who you know: Inferring user profiles in online social networks” (WSDM 2010)
  - Big idea: perform community detection
    - Users are clustered around attribute-based communities
    - Hence, if we find communities, we can infer attributes for users who do not share attributes, based on the fraction of users who do
Community Detection

- Inter-community edges more common than intra-community edges (more than expected by, say, a random distribution of edges)

- Sample algorithm: remove edges that are on the most common shortest paths between any two vertices
Community Detection: Results

**Undergraduates**

![Graph showing normalized mutual information for undergraduates.]

Figure 1: Normalized mutual information versus the fraction of users who reveal their community for Rice undergraduates. Revealing more information naturally leads to partitionings with higher correlations, especially for the college and year attributes. This result shows that different attributes can be accurately inferred with as few as 20% of users revealing their attributes.

**Graduate Students**

![Graph showing normalized mutual information for graduate students.]

Figure 2: Normalized mutual information versus the fraction of users who reveal their community for Rice graduate students.
More sophisticated inferences

Not all friends are equal

  – Privacy can be lost because your friends may have different, laxer, disclosure policy. Use the most restrictive of the pair.

• Inference:
  – Don’t just use friend-links, but also weight friends (based on activity, number of mutual friends)
  – Use wall content text, to further classify users.
Unfriendly: Inference models

Fig. 1. Classification models for inference. Relationships and wall posts leaked by friends can be used to determine properties about the user $w$. These values can then be weighted based on the number of mutual friends or the frequency of communication between two friends.
Unfriendly: Attribute Disclosure versus Attribute Correlation

![Graph showing correlation between attributes for Network A and Network B.](image)
### Unfriendly: Inference results

<table>
<thead>
<tr>
<th>Profile Attribute</th>
<th># of Labels</th>
<th>Baseline</th>
<th>Friend</th>
<th>Wall Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td>2</td>
<td>61.91%</td>
<td>67.08%</td>
<td>76.29%</td>
</tr>
<tr>
<td>Political Views</td>
<td>6</td>
<td>51.53%</td>
<td>58.07%</td>
<td>49.38%</td>
</tr>
<tr>
<td>Religious Views</td>
<td>7</td>
<td>75.45%</td>
<td>83.52%</td>
<td>53.80%</td>
</tr>
<tr>
<td>Relation Status</td>
<td>7</td>
<td>39.45%</td>
<td>45.68%</td>
<td>44.24%</td>
</tr>
<tr>
<td>Favorite Music</td>
<td>604</td>
<td>30.29%</td>
<td>43.33%</td>
<td>-</td>
</tr>
<tr>
<td>Favorite Movies</td>
<td>490</td>
<td>44.30%</td>
<td>51.34%</td>
<td>-</td>
</tr>
<tr>
<td>Favorite TV Shows</td>
<td>205</td>
<td>59.19%</td>
<td>66.08%</td>
<td>-</td>
</tr>
<tr>
<td>Favorite Books</td>
<td>173</td>
<td>42.23%</td>
<td>44.23%</td>
<td>-</td>
</tr>
</tbody>
</table>

**Table 3.** Classifier accuracy for profiles with more than 50 privacy conflicts, representing the upper 25% of our data set. Classifiers using leaked private information consistently outperforms the baseline.
463.2.3 Privacy Risks
Privacy Risks: Attribute Disclosure

- Gaydar: Facebook friendships expose sexual orientation
Privacy Risks:

• New breed of lenders use Facebook and Twitter data to judge borrowers
  – “It’s the whole mantra, birds of a feather tend to flock together. And if you tend to connect with people who are high risk or higher risk borrowers, then the perception is that you are as well. And that’s really where the issue lies.”

• Some startups have advocated using it to approve loans to otherwise risky borrowers
Reading


Discussion Questions

1. How can social networks be best used by advertisers? (Think like an advertiser or social network vendor)

2. Are there alternative approaches to social networking that may limit inference of attributes about users? (Consider architecture, business models, regulation, etc.)