User-Controllable Privacy: An Oxymoron?

Norman Sadeh
Director, Mobile Commerce Lab.
Professor, School of Computer Science
Carnegie Mellon University
www.normsadeh.org
Outline

- Some initial observations
- Identifying Settings/Choices that Matter
  - Quantifying Expressiveness
  - Learning User-Oriented Personas
- The Power of Feedback
- The Power of Suggestions & Dialogues
- Towards Personalized Privacy Assistants: Ongoing research
Privacy Policies

How many of you have read a privacy policy in the last month?
A Quick Off-the-Cuff Estimate

"We estimate that if all American Internet users..."...even after reading the policies, many still can’t answer basic questions...

Privacy Settings: The Illusion of Control

How Tags Work

- **Profile Review** of posts friends tag you in before they go on your profile (note: tags may still appear elsewhere on Facebook)
- **Tag Review** of tags that friends want to add to your posts
- **Maximum Profile Visibility** of posts you're tagged in once they're on your profile
- **Tag Suggestions** when friends upload photos that look like you
- **Friends Can Check You Into Places** using the mobile Places app

Copyright © Norman Sadeh, 2005-2012
Even Worse on Cell Phones
Interview Findings

- Users do not understand Android permissions.
- Largely, the permissions are ignored, with participants instead trusting word of mouth, ratings, and Android market reviews.

Is User-Controllable Privacy an Oxymoron?
At the end of the day, ...

...there are just ...

...we just don’t have the **time/cognitive resources** to make informed decisions of these apps and services
What Would it Take to Empower Users?

- What does it take to capture people’s privacy preferences?
  - Do people even know their privacy preferences?
  - Do these preferences change?
  - Can we simplify the number and types of privacy decisions users have to make?
  - Can we learn people’s privacy preferences?
  - ...and more...
Location Sharing as an Example

- Foursquare-style location sharing ("check-in") only represents a small percentage of scenarios

- Vast majority of utility-based location sharing can’t be supported with push-based ("check-in") model
  - Need to capture people’s location sharing preferences
Locaccino

- More expressive privacy settings
  - “My colleagues can only see my location when I’m on campus and only weekdays 9am-5pm”

- Invisible button

- Auditing functionality

- Available on Android Market, Apple App Store, Ovi, Amazon, etc.

- Tens of thousands of downloads

www.locaccino.org

Copyright © Norman Sadeh, 2005-2012
<table>
<thead>
<tr>
<th>Group</th>
<th>Sharing Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collaborators, Sponsors and Journalists</td>
<td>Collaborators etc. (Jianwei, Ziv and 1 other) can see your location when you are at CMU Campus, on weekdays between 11:00 am and 1:00 pm</td>
</tr>
<tr>
<td>Linda: CMU campus weekdays</td>
<td>Linda (Linda) can see your location when you are at CMU Campus, on weekdays between 8:30 am and 6:00 pm</td>
</tr>
<tr>
<td>Locaccino Faculty</td>
<td>Locaccino Faculty (Jason, Lorrie and 3 others) can see your location when you are at CMU campus or at Lisbon, on weekdays between 8:00 am and 6:00 pm</td>
</tr>
<tr>
<td>Locaccino Group</td>
<td>Locaccino Developers (Paul, Guo and 5 others), Jiali, Rebecca, Michael, Jianwei, Eran, Justin, Jay, Guo and Jonathan can see your location when you are at CMU Campus, on weekdays between 8:00 am and 6:00 pm</td>
</tr>
<tr>
<td>Patricia</td>
<td>Patricia can see your location wherever you are, at all times</td>
</tr>
<tr>
<td>PhD Students</td>
<td>PhD Students (Patrick, Justin and 3 others) can see your location when you are at Some place, on weekdays between 8:00 am and 6:00 pm</td>
</tr>
<tr>
<td>Zipano</td>
<td>P-Air can see your location wherever you are, on weekdays between 8:00 am and 8:00 pm</td>
</tr>
</tbody>
</table>
A First Question

- How much expressiveness to expose to users?

Methodology

- Collect ground truth preferences of (small) representative sample of the population
- Compare how well different combinations of settings capture their preferences
...Rich Preferences...

![Bar chart showing average accuracy for different groups](chart.png)

**Average accuracy**

- Groups: Friends & family, Facebook friends, University community, Advertisers
- Evaluations: Loc/Time, Loc, Time, Time+

Loopt & Latitude: inexpressive settings (mainly “white lists”)

Privacy is Part of the Value Proposition

Users just err on the safe side in setting up their preferences

- More than 2x the sharing with Facebook Friends!
- 2.5 x times the sharing with advertisers!!
With User Burden Considerations – Number of Rules

Average policy accuracy, varying a global limit on number of rules, $c = 20$

- Advertisers
- Facebook friends
- University community
- Friends & family

Legend:
- Loc/Time+
- Loc/Time
- Loc
- Time+
- Time
- White list
Do Users Fully Leverage More Expressive Settings?

- **No:** Depends on the user, the user interface, amount of time, tolerance for error, etc.

- How can we help users make the most of the settings they are given?

- ...Taking into account that we initially have only about 1-2 minutes of their time...
Could Default Policies/Personas Help?

Can You Spot a Good Default Policy?

Green: Share
Red: Don’t

(each square represents a different user)
Introducing Privacy Personas

Generating small numbers of user-understandable privacy profiles ("personas")

Using canonical concepts such as "work", "home", "weekday", "work-hours"

Varying the number of personas presented to users
Do Locations Have Intrinsic Privacy Preferences?

Location entropy as a possible predictor

Can We Entice Users to Tweak their Policies?

Janice Tsai, Patrick Kelley, Paul Hankes Drielsma, Lorrie Cranor, Jason Hong, and Norman Sadeh. 
Who’s Viewed You? The Impact of Feedback in a Mobile-location System. CHI ’09.
Could Auditing Help?

- Users do not always know their own policies
- Users do not fully understand how their rules will operate in practice
- Auditing ('feedback') functionality may help users better understand the behaviors their policies give rise to
Locaccino’s Auditing Functionality

These friends can see your location right now.

Patricia Sadeh
Benefits of Auditing Functionality

Examining Users’ Privacy Rules at the end of the study

Auditing

No Auditing

Average: 122 hr/week

Average: 101 hr/week
Contrast this with Android or the iPhone

Users expected to agree upfront

Coarse 24-hour audit
Can Machine Learning Help?
User-Controllable Policy Learning (patent pending)

- Learning traditionally configured as a “black box” technology
- Users are unlikely to understand the policies they end up with
  - Major source of vulnerability
- Can we develop technology that incrementally suggests policy changes to users?
  - Tradeoff between rapid convergence and maintaining policies that users can relate to


Suggesting Rule Modifications based on User Feedback (patent pending)

Legend:
- Access granted
- Suggested Rule Change
- Audited Request
- Audit says Deny Access
- Audit says Grant Access
Default policies and suggestions can help users make the most of rich settings.
This was just for location...

- How can we scale this to other contextual attributes and more general privacy policies?
- ...on smart phones
- ...with impatient & often distracted users
- ...who are interacting with an ever increasing number of apps and services?
Long-Term Vision: Personalized Privacy Assistants

- Capable of semi-automatically making a number of decisions on behalf of the user
  - Too many decisions otherwise
  - Selectively asks users questions & learns

- Capable of entertaining dialogues to help users understand available options and make better decisions

- Capable of nudging users towards safer practices
How Would this Work?

- Dialogues to identify relevant privacy personas
  - Highlight departures from one’s persona
- Dialogues to evaluate privacy policies
- Dialogues to help configure settings
  - Leverage personas & refined preference models
  - Selectively confirm key decisions
- Dialogues to refine preference models
- Auditing dialogues & even nudging
  - “Did you know that since you installed this app two days ago, ....”
Is User-Controllable Privacy an Oxymoron?
Concluding Remarks

- Privacy is really complex
- Usable privacy is even more complex
- **Short-term:**
  - Expose a limited number of simple decisions
  - Auditing
- **Medium-term:** User-oriented machine learning
- **Longer-term:** towards personalized privacy assistants
- ...May need some help from lawmakers and regulators too
Q&A

mobile commerce lab
Acknowledgements

- Research funded by the US National Science Foundation, the US Army Research Office, Google, CMU CyLab, Google, Nokia, FranceTelecom, ICTI, Microsoft, Pitney Bowes.
References - I


References - II


- J. Cranshaw, E. Toch, J. Hong, A. Kittur, N. Sadeh, "Bridging the Gap Between Physical Location and Online Social Networks", in Proceedings of the Twelfth International Conference on Ubiquitous Computing. Ubicomp 2010

References - III


