# User-Controllable Location Privacy

### Lessons from the Development and Deployment of Location Sharing Apps

Patrick Gage Kelley

Faculty: Norman Sadeh, Lorrie Cranor, Jason Hong Post-Docs: Paul Hankes Drielsma, Eran Toch PhD Students: Jialiu Lin, Janice Tsai, Michael Benisch, Justin Cranshaw, Ram Ravichandran



### **User-Controllable Security & Privacy**

- Users are increasingly expected to set up security and privacy policies:
  - Home computer
  - Flatter, more agile organizations
  - Social networks
- Yet, we know that they have great difficulty doing so
  - Potential vulnerabilities
- Can we develop solutions that help them?

### Mobile Social Networking Apps As a Case Study

- Desire to share data with others
- Mitigated by privacy concerns
- Location sharing as a "hot" application
  - Tens of apps over the past several years
  - ...but adoption has been slow

### **Location Sharing Technologies**



# LOCACCINO

- Gives us access to detailed usage data
- Allows us to experiment with different technologies
- Several thousand downloads over the past year
- Departs from commercial apps:
  - More expressive privacy settings
  - Auditing functionality
  - New technologies (e.g. UCPL)
- Available on Android Market and Nokia Ovi store

### **Ongoing Work**

- **Canonical default policies** can help reduce user burden
- Designing expressive security and privacy policies
  - Explains in part the slow adoption of today's location sharing apps
- User Controllable Policy Learning offers the promise of reconciling the benefits of machine learning with the need for users to remain in charge
- Nudging Users towards safer practices

### Can You Find a Default Policy?

 Location sharing with members of the campus community – 30 different users



### Methodology for Designing Expressive Policies

- Collect ground truth preferences for a representative sample of the user populations
- For different levels of expressiveness, compute the expected efficiency of the policies users would be able to define
  - Assume rational users
  - Search algorithm to identify optimal policies
  - Select among different levels and types of expressiveness based on the above

# **Types of Restrictions**



- Granularity (11.2%)
- Blacklist (15.7%)

Invisible (33.7%)

 Google Latitude

 Friends
 Add friends
 Privacy

 Location sharing
 Output
 Output
 Output

 O Detect your location Learn more Your location is updated automatically
 Output
 Output

#### « Return to friends list

#### % of applications

# **Privacy Controls**

- Best mitigate the greatest expected risks
  - Blacklist (16%)
  - Granularity (12%)
  - Group-based rules (12%)
  - Location-based rules (1%)
  - Time-based rules (1%)

% of applications



### Average Time Shared with Various Groups, Determined by Settings



### User-Controlled 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

### User-Controlled Policy Learning (patent pending)



### **Future Work**

#### Nudging Users towards safer practices

- "Soft paternalism"
- Can we provide users with feedback that nudges them towards safer practices
- Can we identify default policies that are biased towards safer practices?
- How do users respond to this in practice?
- Joint work with Alessandro Acquisti and Lorrie Cranor

### **Expressiveness in Location Sharing**

- Users have complex privacy preferences
  - Simple "white list" approaches only capture a small fraction of scenarios
  - Application becomes less useful: users err on the safe side -> little sharing
  - Time and location are important attributes
    - Other attributes still to be quantified
- Default policies are not easy to find but can help



Research funded by the US National Science Foundation, the US Army Research Office, CMU CyLab, Microsoft, Google, Nokia, FranceTelecom, and ICTI

The User-Controllable Privacy Platform on top of which Locaccino is built is now commercialized by Zipano Technologies.



### **Selection of References**

- Norman Sadeh, Jason Hong, Lorrie Cranor, Ian Fette, Patrick Kelley, Madhu Prabaker, and Jinghai Rao. <u>Understanding and Capturing People's Privacy Policies in a Mobile Social Networking</u> <u>Application</u> Journal of Personal and Ubiquitous Computing 2008.
- Ramprasad Ravichandran, Michael Benisch, Patrick Gage Kelley, and Norman M. Sadeh. <u>Capturing</u> <u>Social Networking Privacy Preferences: Can Default Policies Help Alleviate Tradeoffs between</u> <u>Expressiveness and User Burden?</u> *PETS '09*.
- Janice Tsai, Patrick Kelley, Paul Hankes Drielsma, Lorrie Cranor, Jason Hong, and Norman Sadeh. <u>Who's Viewed You? The Impact of Feedback in a Mobile-location System.</u> *CHI '09*.
- Patrick Kelley, Paul Hankes Drielsma, Norman Sadeh, Lorrie Cranor. <u>User Controllable Learning of</u> <u>Security and Privacy Policies</u>. AISec 2008.
- Michael Benisch, Patrick Gage Kelley, Norman Sadeh, Tuomas Sandholm, Lorrie Faith Cranor, Paul Hankes Drielsma, Janice Tsai. <u>The Impact of Expressiveness on the Effectiveness of Privacy</u> <u>Mechanisms for Location Sharing.</u> CMU-ISR Tech Report 08-141.
- Jason Cornwell, Ian Fette, Gary Hsieh, Madhu Prabaker, Jinghai Rao, Karen Tang, Kami Vaniea, Lujo Bauer, Lorrie Cranor, Jason Hong, Bruce McLaren, Mike Reiter, and Norman Sadeh. <u>User-</u> <u>Controllable Security and Privacy for Pervasive Computing.</u> The 8th IEEE Workshop on Mobile Computing Systems and Applications (HotMobile 2007). 2007.
- Norman Sadeh, Fabien Gandon and Oh Buyng Kwon. <u>Ambient Intelligence: The MyCampus</u> <u>Experience</u> School of Computer Science, Carnegie Mellon University, Technical Report CMU-ISRI-05-123, July 2005.



#### http://cups.cs.cmu.edu

## Patrick Gage Kelley

patrickgage.com me@patrickgage.com twitter.com/patrickgage

with Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor

#### Acknowledgments:

Janice Tsai, Sungjoon Steve Won, Robert Reeder, Aleecia McDonald, Daniel Rhim, Steve Sheng, PK, Robert McGuire, Cristian Bravo-Lillo, Norman Sadeh, Clare-Marie Karat