Understanding and Capturing People's Privacy Preferences in a Friend Finder Application

Norman M. Sadeh - www.cs.cmu.edu/~sadeh

Director, Mobile Commerce Lab – mcom.cs.cmu.edu

School of Computer Science

Carnegie Mellon University

Collaborators: Jason Hong, Lorrie Cranor, Paul Hankes Drielsma, Patrick Kelley, Jialiu Lin, Janice Tsai, Jinghai Rao, Madhu Prabaker

Privacy in Mobile & Pervasive Computing

- **MyCampus** project over the past 7 years
  - Piloted a number of context-aware applications on campus
  - Privacy as a major impediment to adoption
- Wikipedia's definition of privacy: "… the ability of an individual or group to keep their lives and personal affairs out of public view, or to **control the flow of information about themselves**. Privacy is the ability of an individual or organization to **reveal oneself selectively**…"

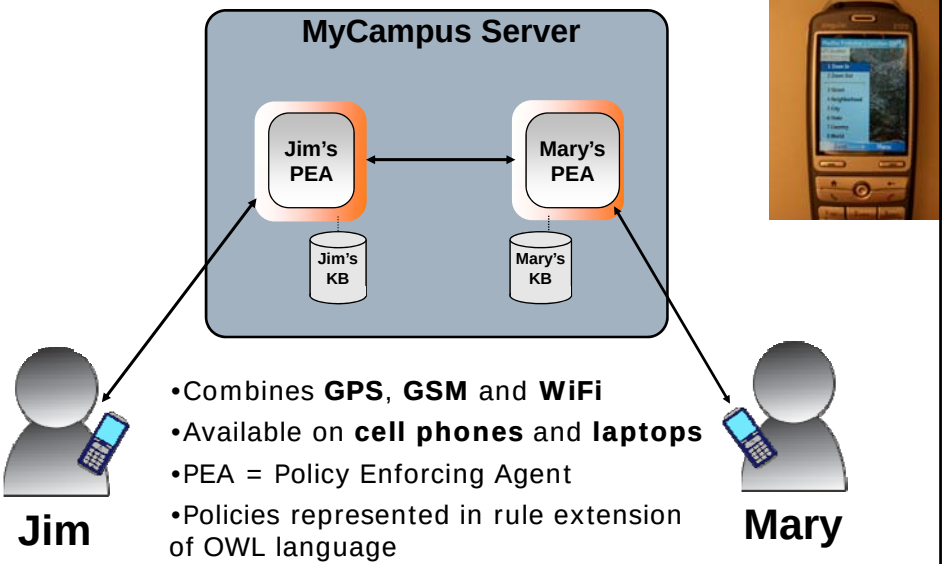
Challenge

- **…But lay users (and even "experts") are not very good at defining privacy policies…**
  - Complexity of people's policies
  - "One size fits all" often doesn't apply
  - Policies change over time
  - Poor understanding of the consequences of how one's information will be used
  - Trust Engine technologies are ahead of usability research

Question

- Can we develop technologies that **empower users** to more accurately specify their policies?
- And some related questions such as:
  - **User burden vs. accuracy**
    - **Incl. expressiveness issue**
  - How does this change **from one application to another**, **from one user to another**?

People Finder Architecture

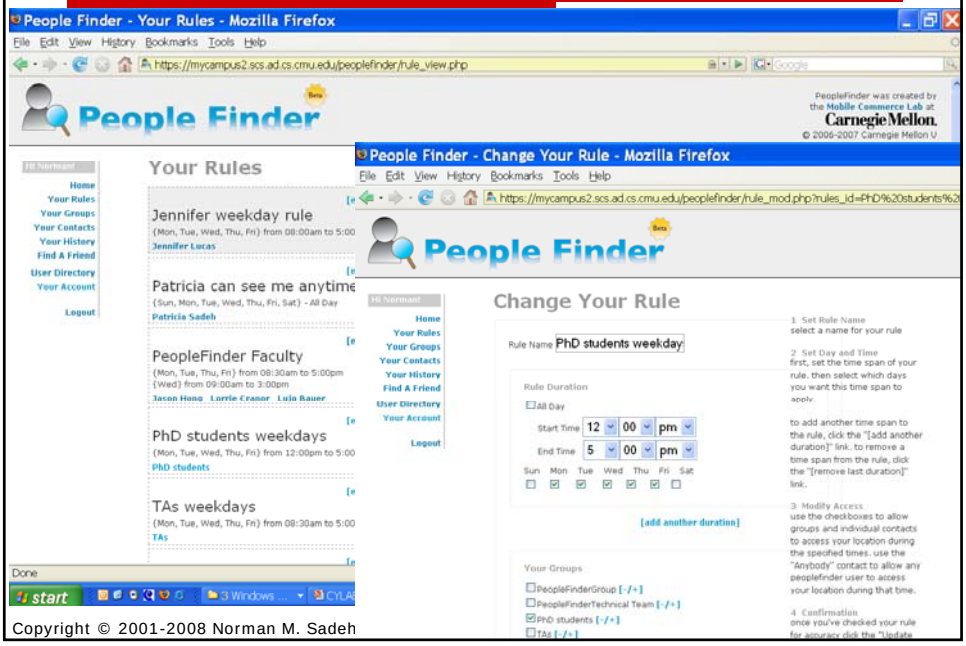


- Combines **GPS**, **GSM** and **WiFi**
- Available on **cell phones** and **laptops**
- PEA = Policy Enforcing Agent
- Policies represented in rule extension of OWL language

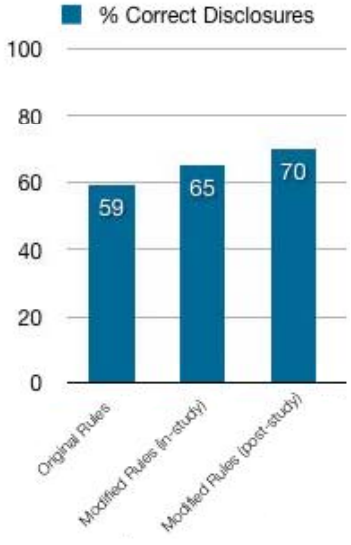
People's Policies Are Often Varied & Complex

- User's willingness to share their location depends on:
  - Who is asking
  - When
  - Where they are
  - What they are doing
  - Who they are with
  - And more…

People Finder – Defining Rules



Users Are Not Good At Defining Policies

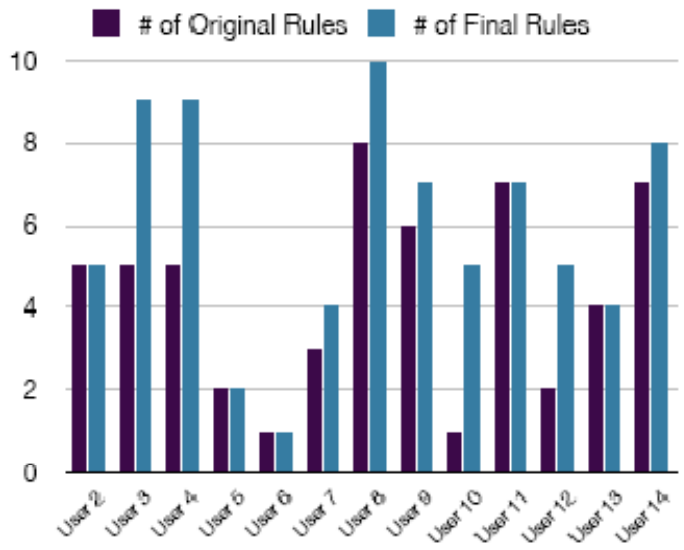


People Finder Application:

- Lab study with 19 users
- 30 queries per user

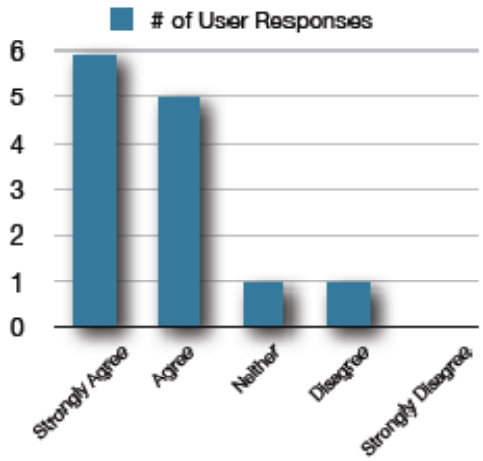
	Mean (sec)	Standard Deviation (sec)
Rule Creation	321.53	206.10
Rule Maintenance	101.15	110.02
Total	422.69	213.48

…and it's not for lack of trying…

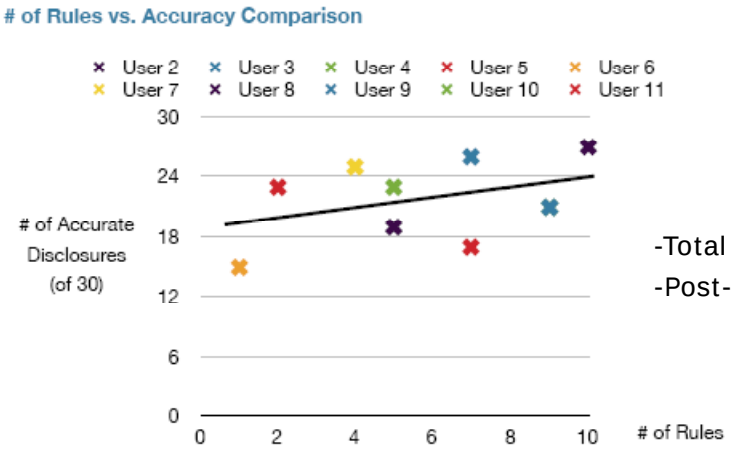


It's Not Because of the Interface

Modifying rules was easy using the system's rule interface



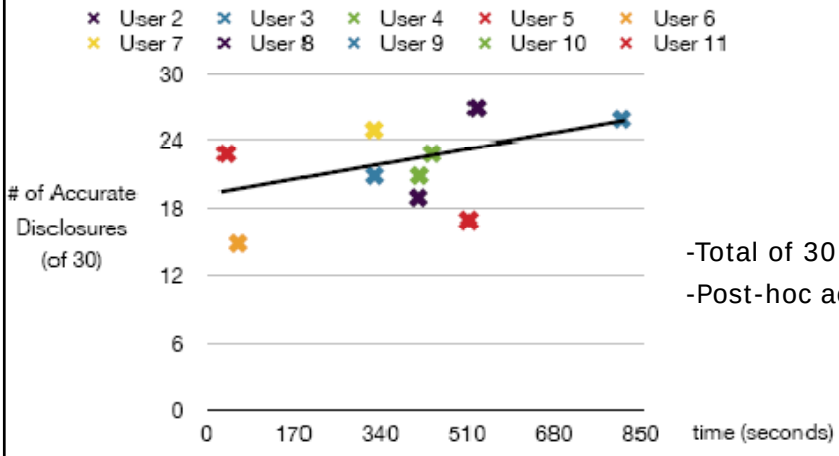
Only Slight Correlation with # Rules



-Total of 30 requests
-Post-hoc accuracy

Regression Line	R-squared
y = 0.4789x + 18.876	R2 = 0.1397

Only Slight Correlation with Time Spent



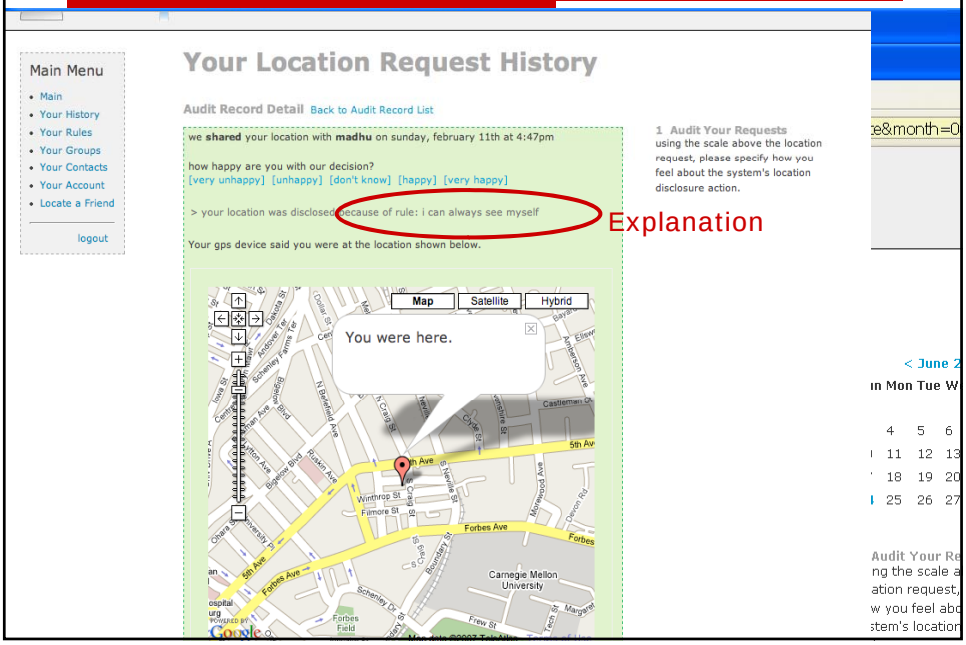
-Total of 30 requests
-Post-hoc accuracy

Regression Line	R-squared
y = 0.0076x + 18.698	R2 = 0.2031

Importance of Feedback - Notifications

PeopleFinder application

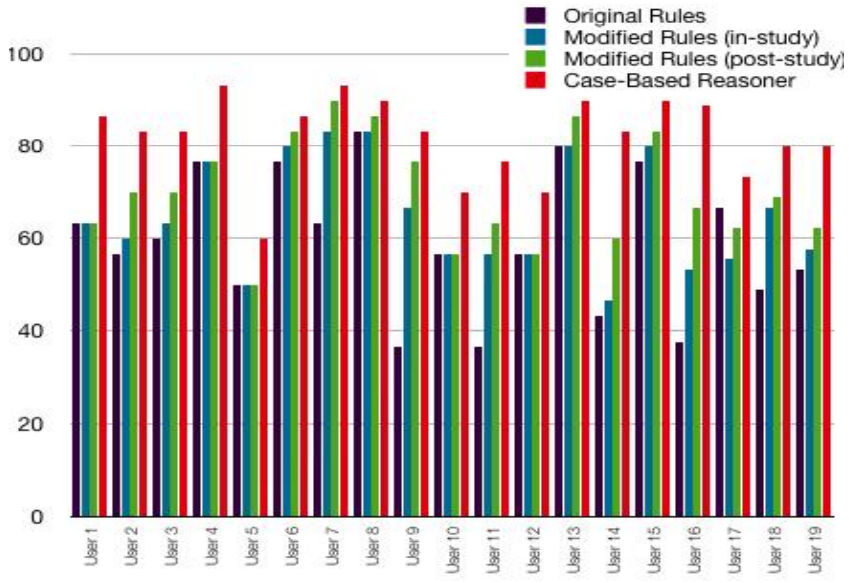
Feedback Through Audit Logs



Machine Learning

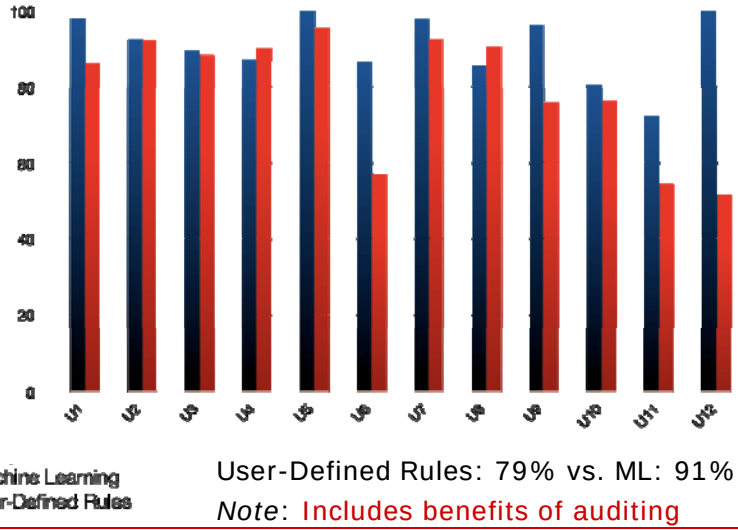
- Audited Logs can be used to refine a user's policies

Lab Study



More Recent Pilots – 12 most active target users

3 Pilots – total of over 60 participants



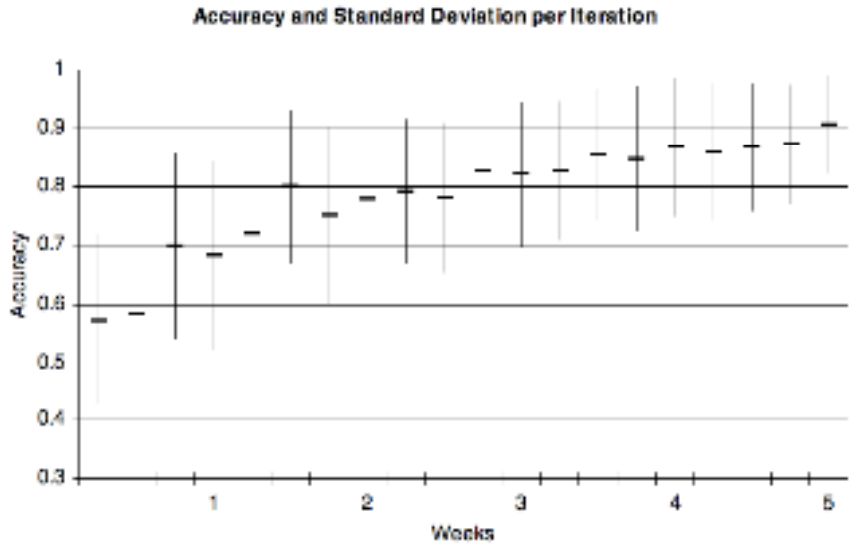
User-Defined Rules: 79% vs. ML: 91%

Note: Includes benefits of auditing

User-Controllable Policy Learning

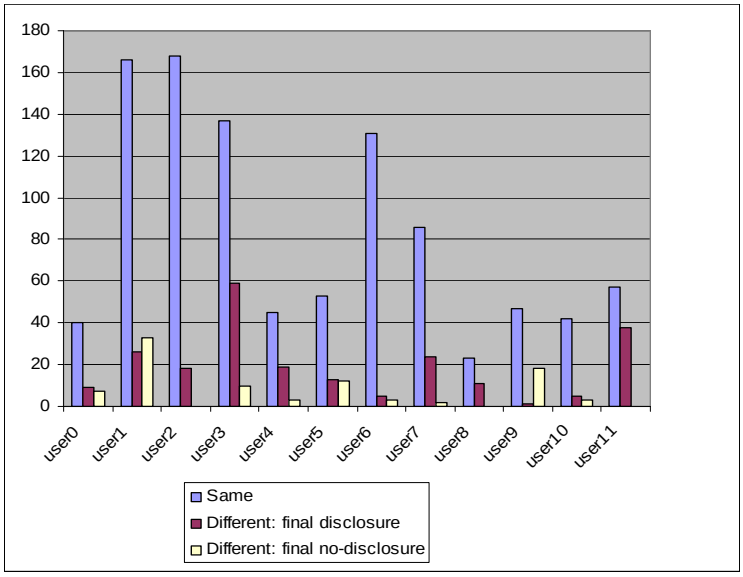
- Learning is a "black box" technology
  - Users are unlikely to understand the policies they end up with
  - Source of vulnerability
- Can we develop technology that incrementally suggests policy changes to users?
  - User remains in control

New Family of User-Controllable Policy Learning Techniques (Patent Pending)



Human-understandable suggestions help improve user-defined policies

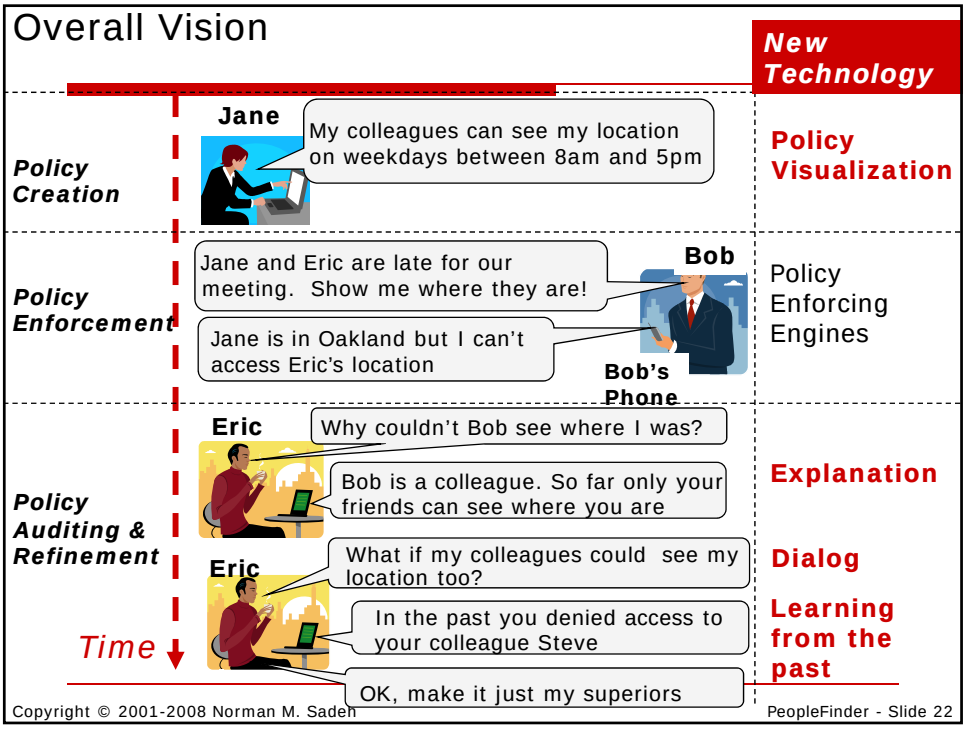
Policy Evolution



Other Promising Approaches

- Visualization Techniques
- Explanations & dialogues

Overall Vision



Some of the Things We've Learned So Far

- Adoption will depend on whether users feel they have **adequate control** over the disclosure of their contextual information
- People often have rather complex privacy preferences
  - People are **not good at specifying their policies**
  - Not easy to identify good **default policies** beyond just **denying all requests**
- Policies tend to become **more complex as users grow more sophisticated**
  - Allowing more requests but in an increasingly selective way
- **Auditing** is critical
  - **Learning, explanation & dialogues make a difference**
- **Applies to <u>both</u> privacy and security policies**

 PeopleFinder - Slide 23

Q&A

 PeopleFinder - Slide 24

Some References

- User-Controllable Security and Privacy Project:
  http://www.cs.cmu.edu/%7Esadeh/user_controllable_security_and_privacy.htm
- Norman Sadeh, Fabien Gandon and Oh Buyng Kwon, "Ambient Intelligence: The MyCampus Experience", Chapter in "Ambient Intelligence and Pervasive Computing", Eds. T. Vasilakos and W. Pedrycz, ArTech House, 2006. (Also available as Tech. Report CMU-ISRI-05-123, School of Computer Science, Carnegie Mellon University) -
  http://www.cs.cmu.edu/%7Esadeh/Publications/More%20Complete%20List/Ambient%20Intelligence%20Tech%20Report%20final.pdf
- Jason Cornwell, Ian Fette, Gary Hsieh, Madhu Prabaker, Jinghai Rao, Karen Tang, Kami Vaniea, Lujo Bauer, Lorrie Cranor, Jason Hong, Bruce McLaren, Mike Reiter, Norman Sadeh, "User-Controllable Security and Privacy for Pervasive Computing", Proceedings of the 8th IEEE Workshop on Mobile Computing Systems and Applications (HotMobile 2007), February 2007.
  http://www.cs.cmu.edu/%7Esadeh/Publications/More%20Complete%20List/HotMobile2007-user-controllable-security-privacy%20submitted%20FINAL.pdf
- M. Prabaker, J. Rao, I. Fette, P. Kelley, L. Cranor, J. Hong, and N. Sadeh, "**Understanding and Capturing People's Privacy Policies in a People Finder Application**", 2007 Ubicomp Workshop on Privacy, Austria, Sept. 2007

