



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 Hanks 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

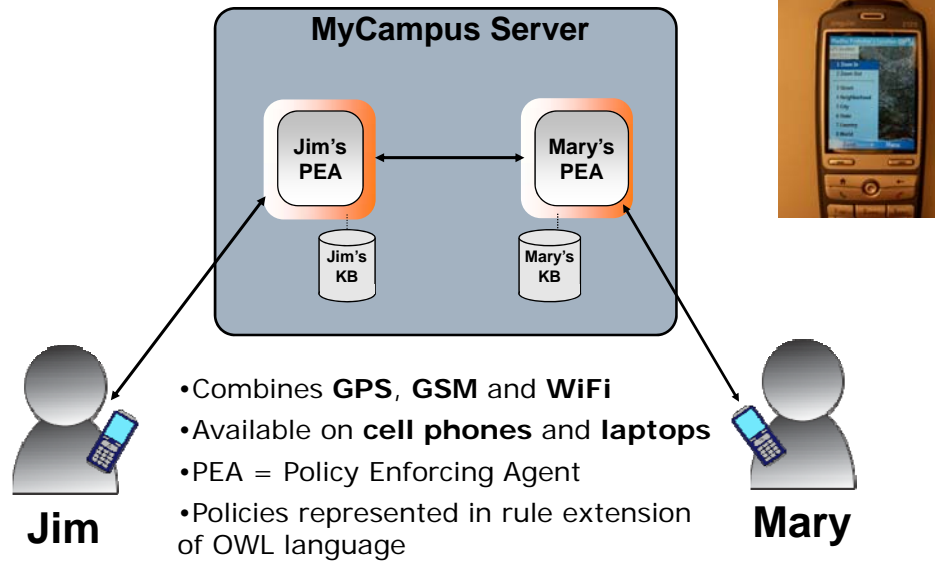
- ...But lay users (and even “experts”) are not very good at defining privacy policies...
 - Complexity of people’s policies
 - “One size fits all” often doesn’t apply
 - Policies change over time
 - Poor understanding of the consequences of how one’s information will be used
 - Trust Engine technologies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



Copyright © 2001-2008 Norman M. Sadeh

PeopleFinder - Slide 5

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...

Copyright © 2001-2008 Norman M. Sadeh

PeopleFinder - Slide 6



People Finder – Defining Rules

The screenshot displays the 'People Finder - Your Rules' page in a Mozilla Firefox browser. The page lists several rules: 'Jennifer weekday rule', 'Patricia can see me anytime', 'PeopleFinder Faculty', 'PhD students weekdays', and 'TAs weekdays'. A secondary window titled 'Change Your Rule' is open, showing a form for 'PhD students weekday'. The form includes fields for 'Rule Name', 'Rule Duration' (with 'All Day' selected), 'Start Time' (12:00 pm), and 'End Time' (5:00 pm). There are also checkboxes for days of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat) and a 'Your Groups' section with checkboxes for 'PeopleFinderGroup', 'PeopleFinderTechnical Team', 'PhD students', and 'TAs'. Instructions on the right side of the form guide the user through the process of setting the rule name, duration, and access permissions.

Copyright © 2001-2008 Norman M. Sadeh

Users Are Not Good At Defining Policies

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

Bar chart data:

Category	% Correct Disclosures
Original Rules	59
Modified Rules (in-study)	65
Modified Rules (post-study)	70

People Finder Application:

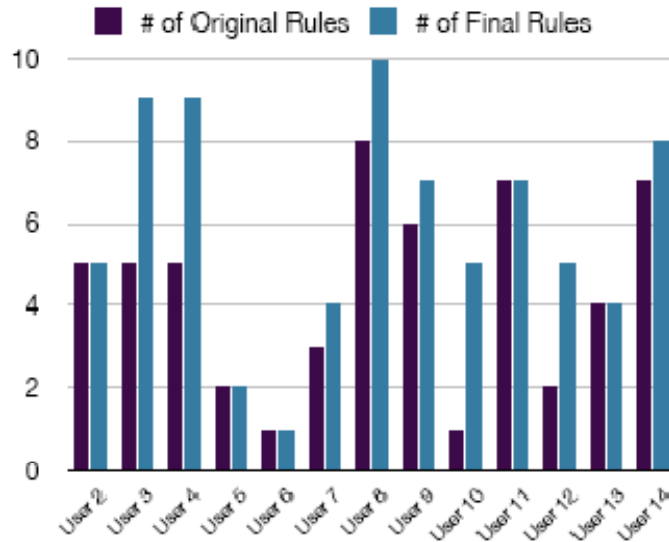
- Lab study with 19 users
- 30 queries per user

Copyright © 2001-2008 Norman M. Sadeh

PeopleFinder - Slide 8



...and it's not for lack of trying...

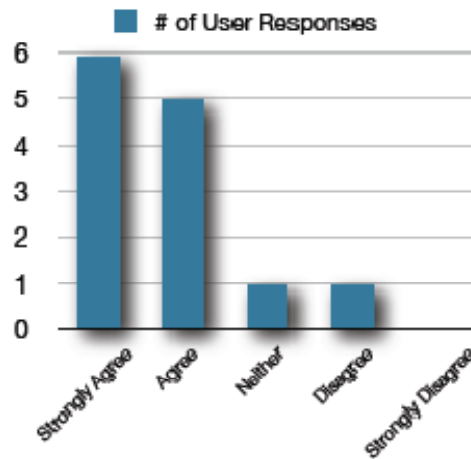


Copyright © 2001-2008 Norman M. Sadeh

PeopleFinder - Slide 9

It's Not Because of the Interface

Modifying rules was easy using the system's rule interface



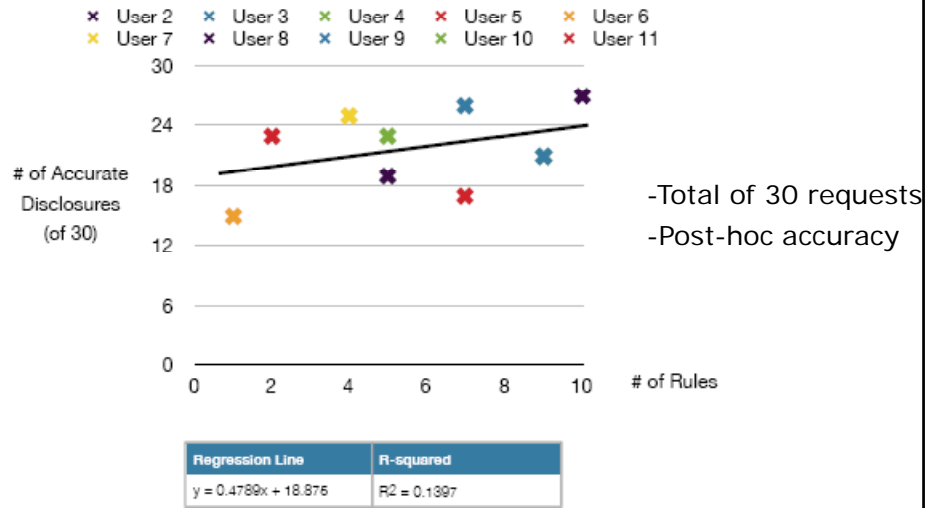
Copyright © 2001-2008 Norman M. Sadeh

PeopleFinder - Slide 10



Only Slight Correlation with # Rules

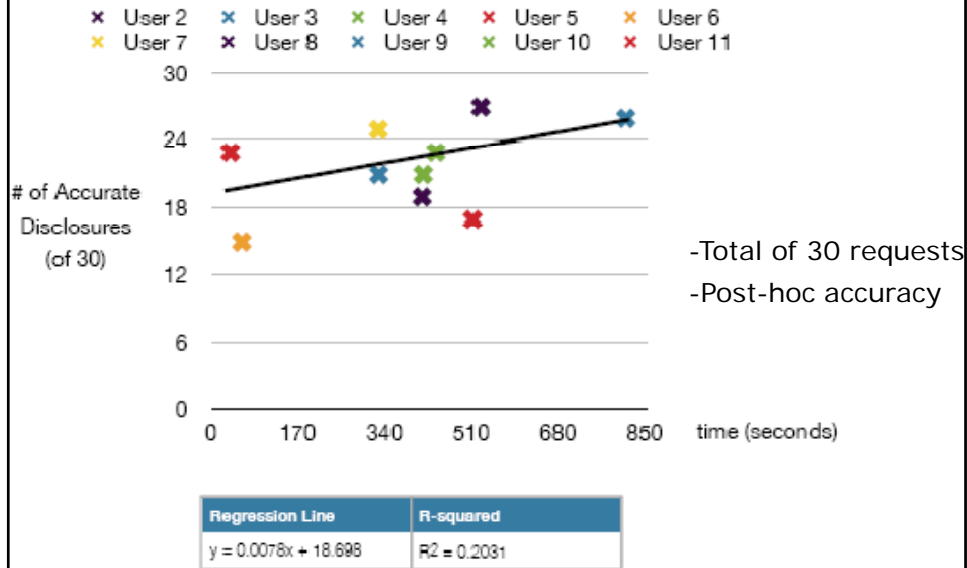
of Rules vs. Accuracy Comparison



Copyright © 2001-2008 Norman M. Sadeh

PeopleFinder - Slide 11

Only Slight Correlation with Time Spent



Copyright © 2001-2008 Norman M. Sadeh

PeopleFinder - Slide 12



Importance of Feedback - Notifications



PeopleFinder application

Feedback Through Audit Logs

Your Location Request History

[Audit Record Detail](#) [Back to Audit Record List](#)

we shared your location with **madhu** on sunday, february 11th at 4:47pm

how happy are you with our decision?
[very unhappy] [unhappy] [don't know] [happy] [very happy]

> your location was disclosed because of rule: i can always see myself

Your gps device said you were at the location shown below.

1. Audit Your Requests using the scale above the location request, please specify how you feel about the system's location disclosure action.

< June 2
in Mon Tue W
4 5 6
11 12 13
18 19 20
25 26 27

Audit Your Re
ng the scale a
ation request,
w you feel abo
stem's location

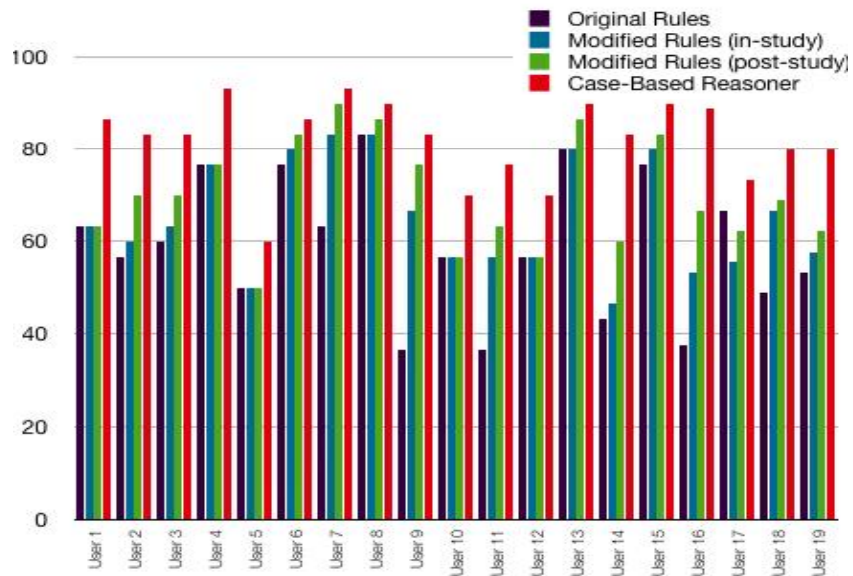
Explanation



Machine Learning

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

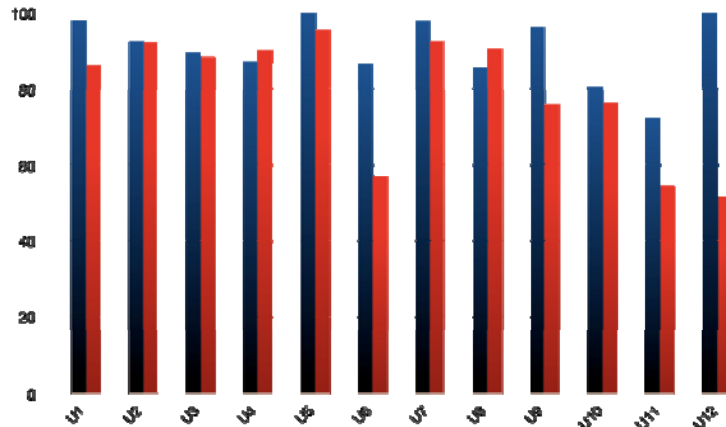
Lab Study





More Recent Pilots – 12 most active target users

3 Pilots – total of over 60 participants



■ Machine Learning
■ User-Defined Rules

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

Note: Includes benefits of auditing

Copyright © 2001-2008 Norman M. Sadeh

PeopleFinder - Slide 17

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

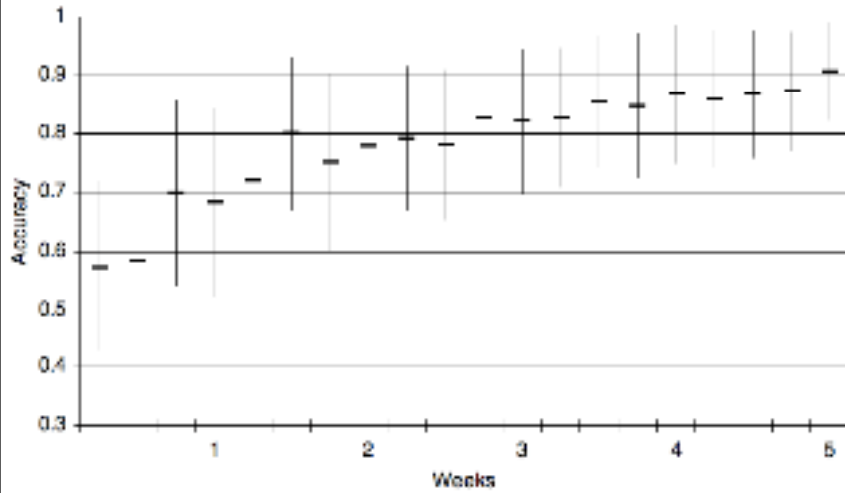
Copyright © 2001-2008 Norman M. Sadeh

PeopleFinder - Slide 18



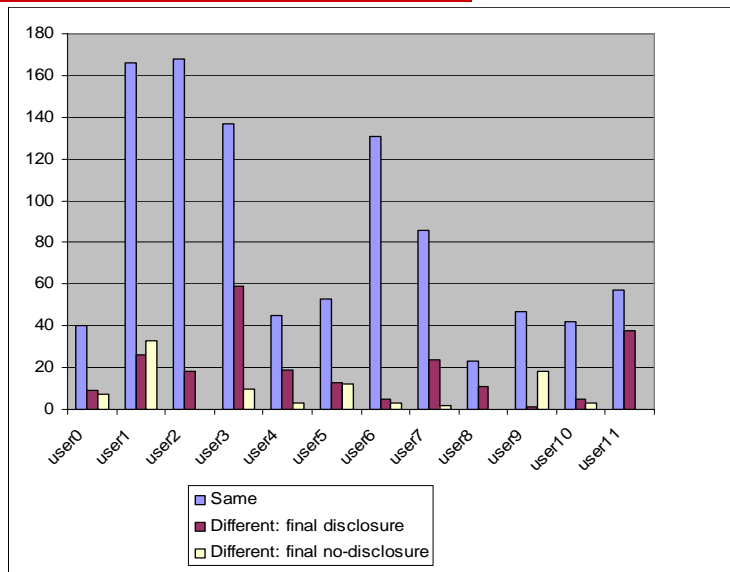
New Family of User-Controllable Policy Learning Techniques (Patent Pending)

Accuracy and Standard Deviation per Iteration



Human-understandable suggestions help improve user-defined policies

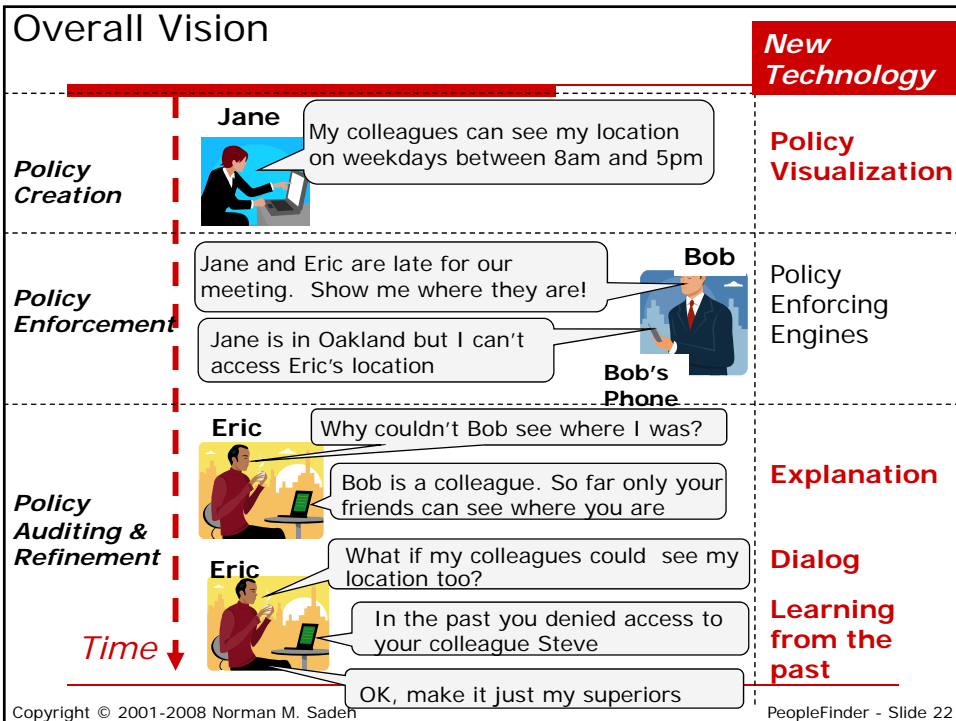
Policy Evolution





Other Promising Approaches

- Visualization Techniques
- Explanations & dialogues





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 **both** privacy and security policies

Q&A



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