

# User-Controllable Privacy and Security for Pervasive Computing



Norman Sadeh, Lujo Bauer, Lorrie Cranor, Jason Hong, Bruce McLaren and Michael Reiter  
 School of Computer Science & CyLab – Carnegie Mellon University

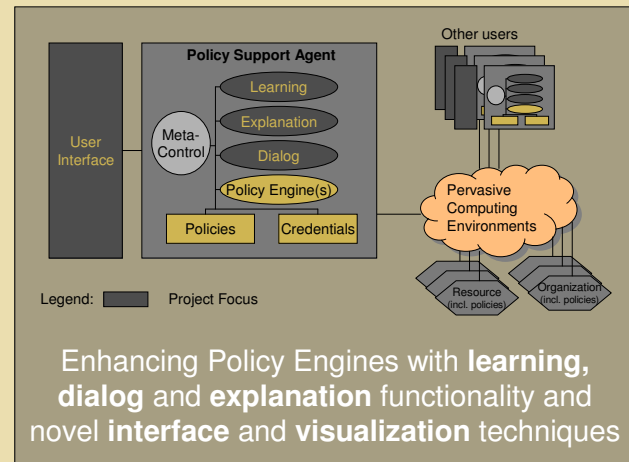
URL: [www.cs.cmu.edu/~sadeh/user\\_controllable\\_security\\_and\\_privacy.htm](http://www.cs.cmu.edu/~sadeh/user_controllable_security_and_privacy.htm) - NSF Award Number: CNS-0627513 (Sept 2006 – Aug 2010)

## CHALLENGE:

- End-users are not good at managing security and privacy policies
- Difficulty of **articulating one's policies and reasoning** about them
- **Mobile and Pervasive computing devices and services** are often **unmanaged** and also entail additional **usability** challenges

## OBJECTIVES:

- Develop and validate techniques to **empower end-users to manage their policies**
- Evaluate **tradeoffs between expressiveness, tolerance for errors, burden on users and overall user acceptance**
- Understand **how much we can realistically hope to delegate to users** – business and policy implications

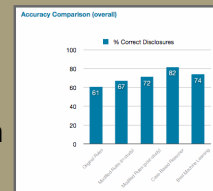


## Sample of Techniques

- **Learning:** Attempt to learn user policies by recording their decisions in a limited number of situations.
- **Conversational User Interfaces:** User dialogs and explanation to help answer “Why?”, “Why not?” and “What if?” questions
- Novel **visualization** and **interface** techniques to help users audit decisions and refine their policies

## Benefits

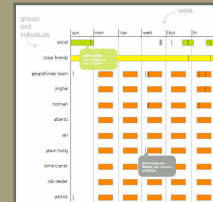
- Experiments suggest that learning can **reduce user burden and improve accuracy**
- Heuristics can be used to transform proofs into simpler, **human-oriented explanations**
- Help users understand the consequences of their policies, **improving accuracy and sense of being in control.**



“...k\_cylab signed (delegate (k\_cylab, k\_cylab.faculty, cic-e2130))...”

↓

“Bob is a student, and Alice allowed students into her office”



## Broader Impact

- The **adoption of a number of mobile and pervasive computing** applications hinges on the ability of users to effectively control associated security and privacy policies
- **Corporations and government organizations** require similar tools to manage an ever expanding range of policies – from **role-based access control** to a variety of **regulations** to **complex inter-organizational interactions**

## Current Application Domains

### Contextual Instant Messenger

Users can automatically inquire about each other's context (interruptability, location, and current task) through an instant messaging service.

### Phone-based People Finder

Users are provided with smartphones that track their location. They interact with their devices to inquire about the locations of others, subject to privacy policies.

### Phone-based Access Control

Smartphones act as tokens by which users access both physical and digital resources. Users use their phones to create and manage their security policies.