

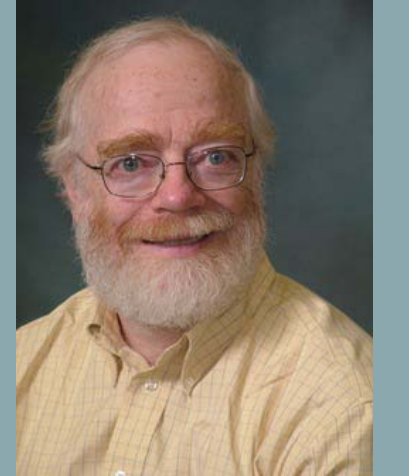
User-Controllable Policy Learning

PIs: **Norman Sadeh** and **Steve Bellovin**

<http://mcom.cs.cmu.edu/user-controllable-policy-learning/>



Norman Sadeh
Carnegie Mellon Univ.



Steve Bellovin
Columbia Univ.

The Challenge:

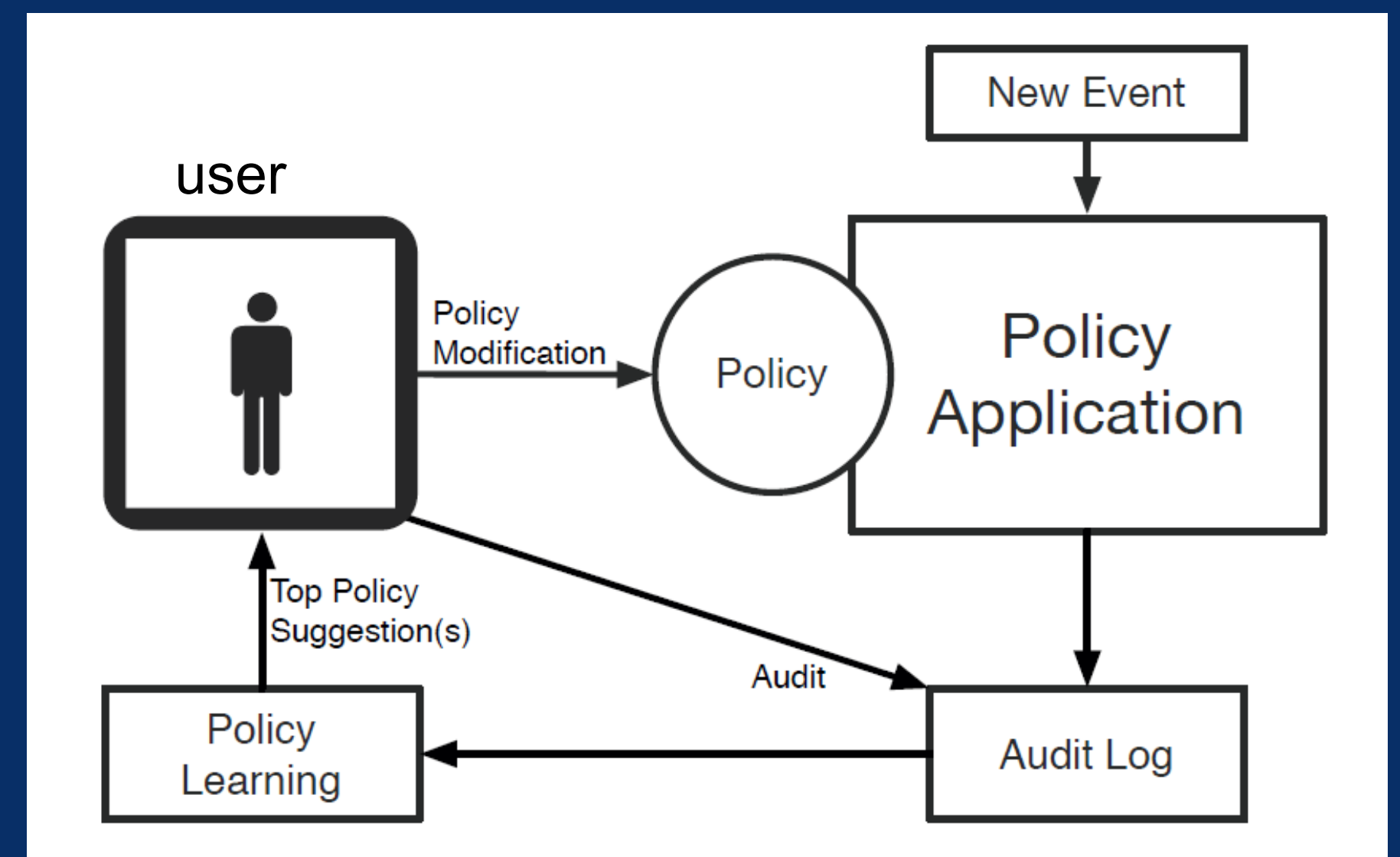
- Users are expected to configure a wide range of security and privacy policies (e.g. smart phones, social networks, RBAC, DLP, firewalls)
- Yet, they have great difficulty doing so because:
 - They don't understand their policies
 - They can't express their policies
 - They don't have the time
 - Their policies change
 - etc.

The Idea:

Can we develop **user-oriented machine learning techniques that empower users to more effectively specify and control their policies?**

Moving away from "black box" configuration of machine learning that take over from the users: **Users need to understand and remain in control of their policies**

Mixed-initiative learning of security and privacy policies



Approach

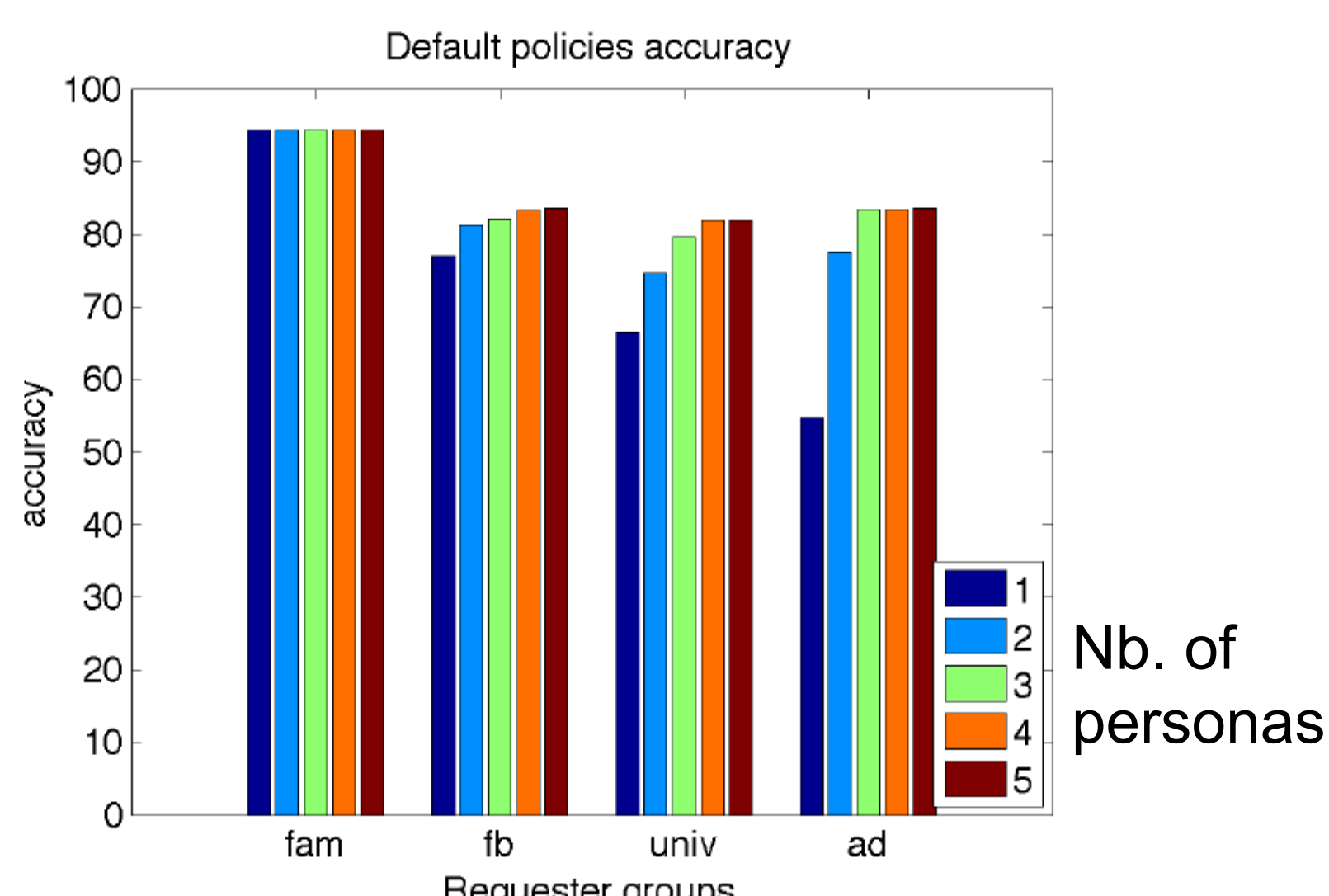
Using Machine Learning to Identify Understandable Privacy/Security Personas

Our research has shown that it is often possible to identify a small number of personas that can help reduce user burden and increase policy accuracy

Using Machine Learning to Suggest Policy Changes to Users

Our research has shown that it is often possible to convert user feedback on the performance of their policy into understandable suggestions for refining these policies

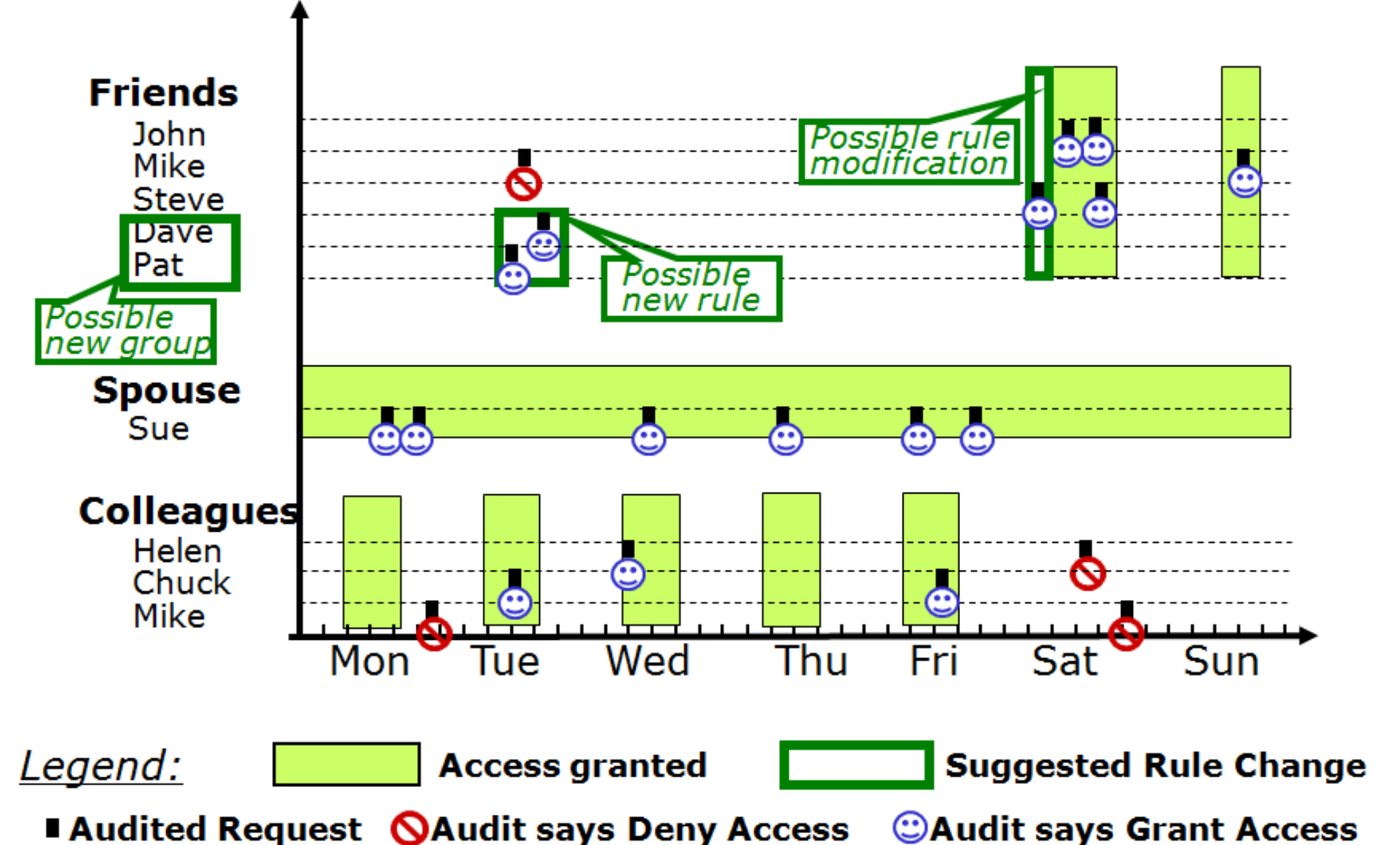
Quantifying the Benefits of Different Numbers of Policy Personas: Location Sharing Privacy Policy Example



Legend: fam=family; fb=Facebook friends; univ=members of the university community; ad= advertisers

Suggesting Refinements to one's Policy: Location Sharing Privacy Policy Example

(patent pending)



Interested in meeting the PIs? Attach post-it note below!



National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD

