

# **User-Controllable Privacy: An Oxymoron?**

---

**Norman Sadeh**

Director, Mobile Commerce Lab.

Professor, School of Computer Science

Carnegie Mellon University

[www.normsadeh.org](http://www.normsadeh.org)



# Outline

---

- Some initial observations
- Identifying Settings/Choices that Matter
  - Quantifying Expressiveness
  - Learning User-Oriented Personas
- The Power of Feedback
- The Power of Suggestions & Dialogues
- Towards Personalized Privacy Assistants: Ongoing research

# Privacy Policies

A screenshot of the Amazon.com Help page. The browser address bar shows the URL www.amazon.com/gp/help/customer/display.html?nodeId=468496. The Amazon logo and navigation links like 'Today's Deals', 'Gift Cards', and 'Help' are visible. A large yellow rectangular box is overlaid on the page, containing the text 'How many of you have read a privacy policy in the last month?'. Below this box, a list of links is visible, including 'What About Cookies?', 'Does Amazon.com Share the Information It Receives?', 'How Secure Is Information About Me?', 'What About Third-Party Advertisers and Links to Other Websites?', and 'Which Information Can I Access?'. A 'Contact Us' button is also present in the bottom right corner.

Amazon.com Help: Pri x

www.amazon.com/gp/help/customer/display.html?nodeId=468496

amazon Prime

Today's Deals | Gift Cards | Help

The All-N

Hello, Norman

Shop by Department

How many of you have read a privacy policy in the last month?

Top

< Privacy Policy

Pro

Co

Su

Re

An

Se

Ou

Yo

A-

Is This E-mail from Amazon?

E-mail Account Verification

Security Researchers and Professionals

- What About Cookies?
- Does Amazon.com Share the Information It Receives?
- How Secure Is Information About Me?
- What About Third-Party Advertisers and Links to Other Websites?
- Which Information Can I Access?

Contact Us

# A Quick Off-the-Cuff Estimate

---

...even after reading  
the policies, many still  
can't answer basic  
questions...

*Policies , Proc. of CH12008.*

# Privacy Settings: The Illusion of Control



## How Tags Work

**Profile Review** of posts friends tag you in before they go on your profile (note: tags may still appear elsewhere on Facebook)

Off >

**Tag Review** of tags that friends want to add to your posts

On >

**Maximum Profile Visibility** of posts you're tagged in once they're on your profile

\* Custom ▾

**Tag Suggestions** when friends upload photos that look like you

No One >

**Friends Can Check You Into Places** using the mobile Places app

Off >

Done

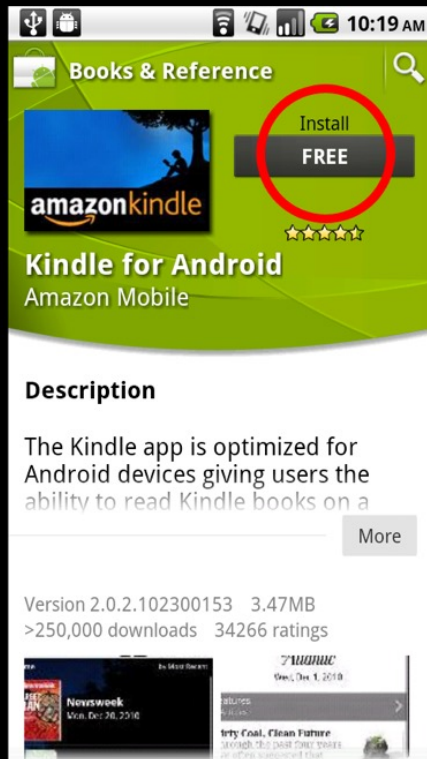
(Offline)

Instant personalization

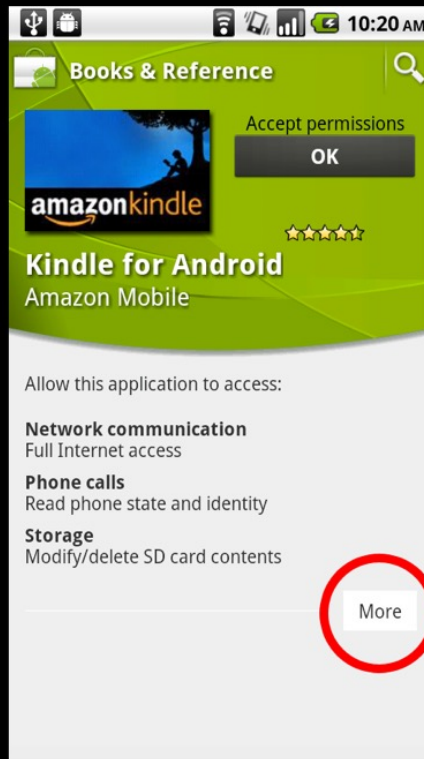
Lets you see relevant information about your friends the moment you arrive on select partner websites.

Edit Settings

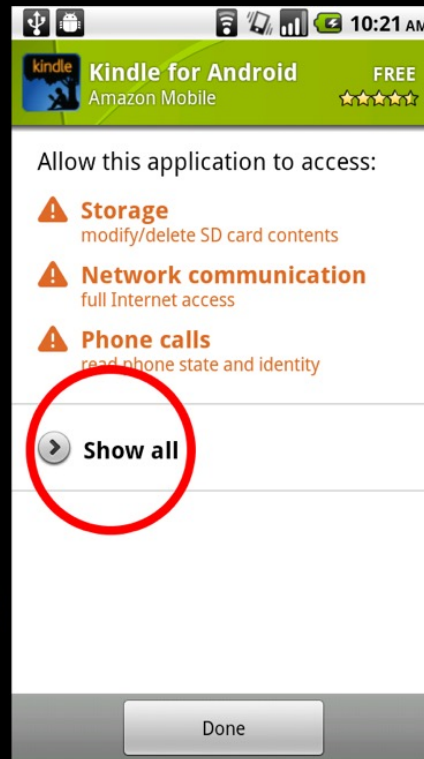
# Even Worse on Cell Phones



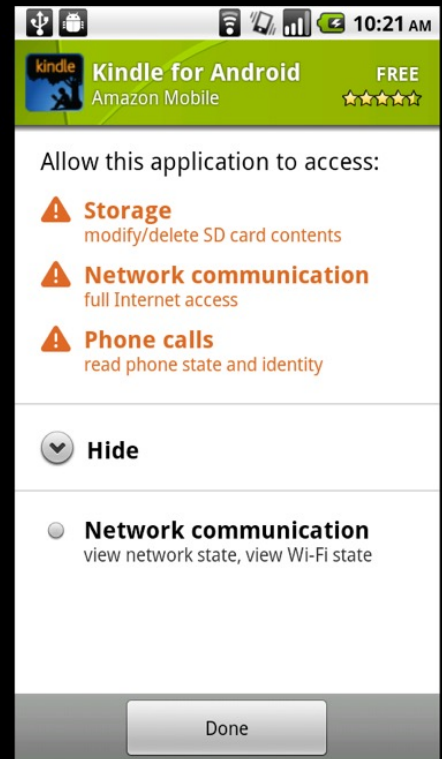
1



2



3



4

# Interview Findings

---

- ❑ Users **do not understand Android permissions.**
- ❑ Largely, the permissions are ignored, with participants instead **trusting word of mouth, ratings, and Android market reviews.**

P. Gage Kelley, S. Consolvo, L. Cranor, J. Jung, N. Sadeh, D. Wetherall, **"A Conundrum of Permissions: Installing Applications on an Android Smartphone"**, USEC2012.

---

# **Is User-Controllable Privacy an Oxymoron?**



At the end of the day, ...

---

there are just

...we just don't have  
the **time/cognitive  
resources** to make  
informed decisions

of these apps and services

# What Would it Take to Empower Users?

---

- ❑ What does it take to capture people's privacy preferences?
  - Do people even know their privacy preferences?
  - Do these preferences change?
  - Can we simplify the number and types of privacy decisions users have to make?
  - Can we learn people's privacy preferences?
  - ...and more...

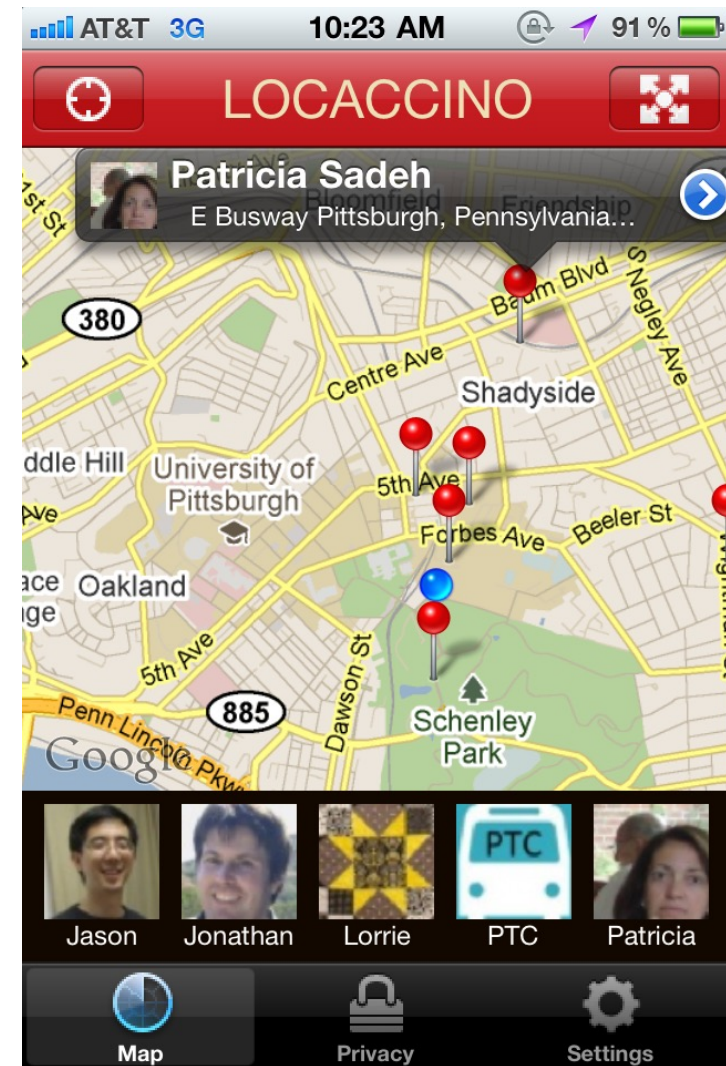
# Location Sharing as an Example

---

- Foursquare-style location sharing (“check-in”) only represents a small percentage of scenarios
- **Vast majority of utility-based location sharing can’t be supported with push-based (“check-in”) model**
  - Need to capture people’s location sharing preferences

# Locaccino

- ❑ **More expressive privacy settings**
  - “My colleagues can only see my location when I’m on campus and only weekdays 9am-5pm”
  - **Invisible button**
- ❑ **Auditing functionality**
- ❑ Available on Android Market, Apple App Store, Ovi, Amazon, etc.
- ❑ Tens of thousands of downloads



[www.locaccino.org](http://www.locaccino.org)

## Location sharing rules

**Collaborators, Sponsors and Journalists**

Collaborators etc. ([Jianwei](#), [Ziv](#) and 1 other) can see your location when you are at **CMU Campus**, on **weekdays** between **11:00 am** and **1:00 pm**

Edit

✕ Delete

**Linda: CMU campus weekdays**

Linda ([Linda](#)) can see your location when you are at **CMU Campus**, on **weekdays** between **8:30 am** and **5:00 pm**

Edit

✕ Delete

**Locaccino Faculty**

Locaccino Faculty ([Jason](#), [Lorrie](#) and 3 others) can see your location when you are at **CMU campus** or at **lisbon**, on **weekdays** between **8:00 am** and **6:00 pm**

Edit

✕ Delete

**Locaccino Group**

Locaccino Developers ([Paul](#), [Guo](#) and 5 others), [Jialiu](#), [Rebecca](#), [Michael](#), [Jianwei](#), [Eran](#), [Justin](#), [Jay](#), [Guo](#) and [Jonathan](#) can see your location when you are at **CMU Campus**, on **weekdays** between **8:00 am** and **6:00 pm**

Edit

✕ Delete

**Patricia**

Patricia can see your location **wherever you are, at all times**

Edit

✕ Delete

**PhD Students**

PhD Students ([Patrick](#), [Justin](#) and 3 others) can see your location when you are at **Some place**, on **weekdays** between **8:00 am** and **6:00 pm**

Edit

✕ Delete

**Zipano**

P-Air can see your location **wherever you are**, on **weekdays** between **8:00 am** and **8:00 pm**

Edit

✕ Delete

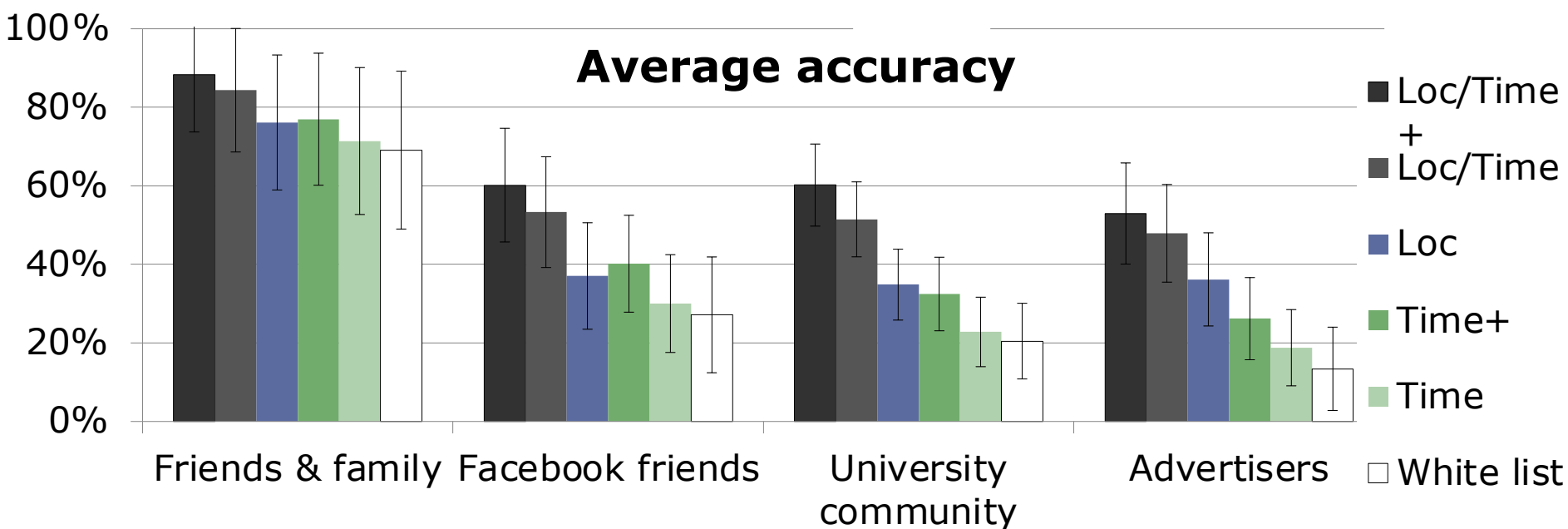
[+ Add New Rule](#)

# A First Question

---

- ❑ **How much expressiveness to expose to users?**
- ❑ **Methodology**
  - Collect ground truth preferences of (small) representative sample of the population
  - Compare how well different combinations of settings capture their preferences

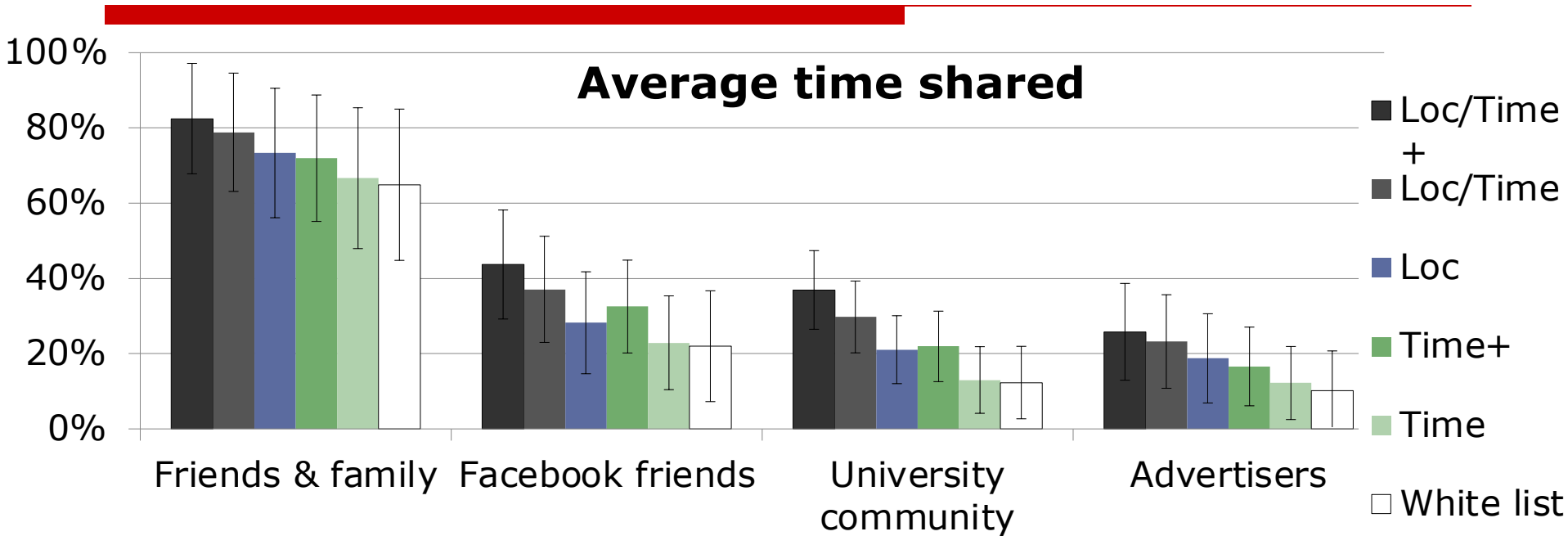
# ...Rich Preferences...



## Loopt & Latitude: **inexpressive settings** (mainly “white lists”)

Michael Benisch, Patrick Gage Kelley, Norman Sadeh, Lorrie Faith Cranor. [Capturing Location Privacy Preferences: Quantifying Accuracy and User Burden Tradeoffs](#). *Journal of Personal and Ubiquitous Computing*, 2011.

# Privacy is Part of the Value Proposition



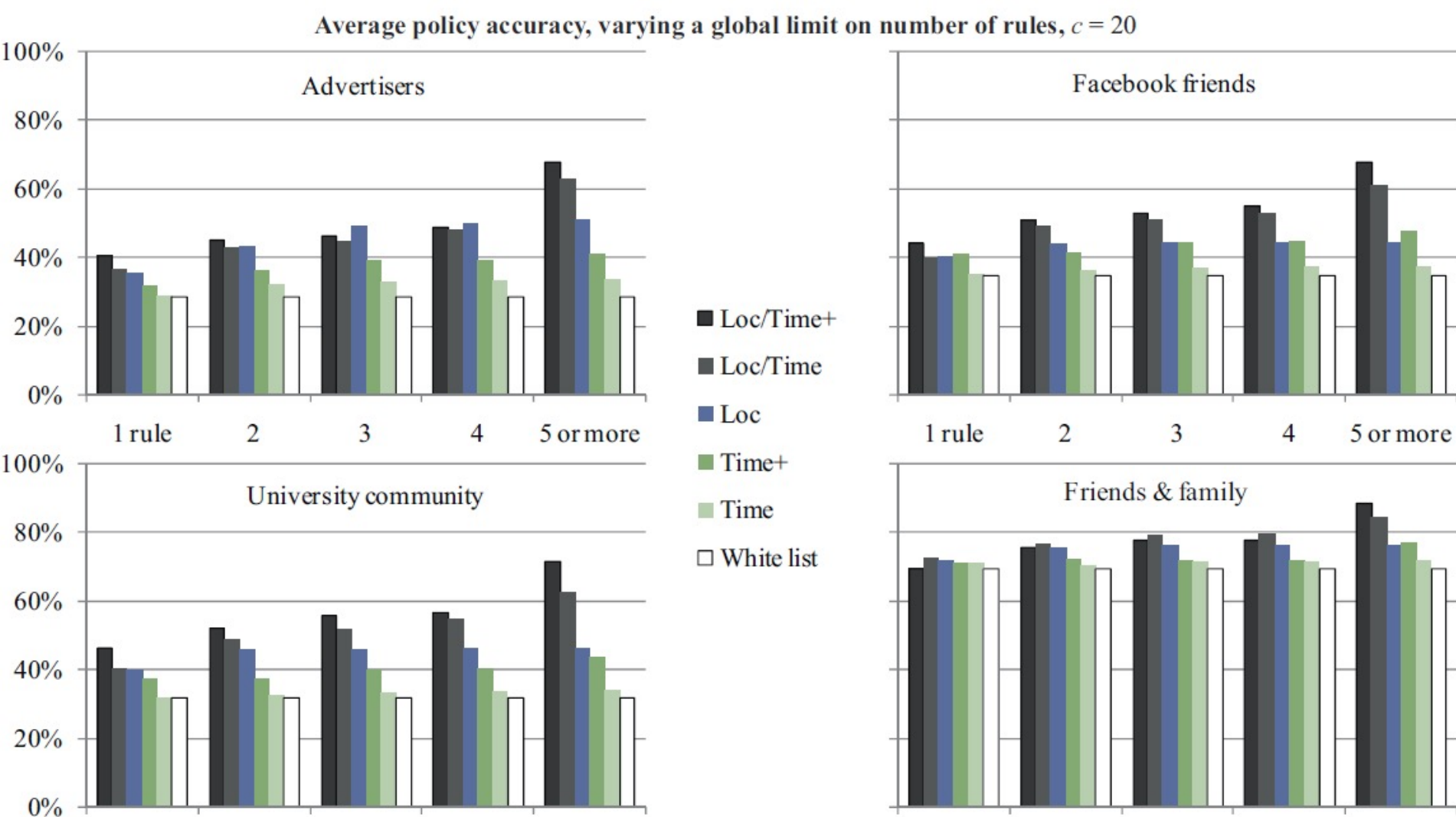
Users just err on the safe side in setting up their preferences

➤ More than 2x the sharing with Facebook Friends!

➤ 2.5 x times the sharing with advertisers!!



# With User Burden Considerations – Number of Rules



# **Do Users Fully Leverage More Expressive Settings?**

- No:** Depends on the user, the user interface, amount of time, tolerance for error, etc.
- How can we help users make the most of the settings they are given?**
- ...Taking into account that we initially have only about 1-2 minutes of their time...**

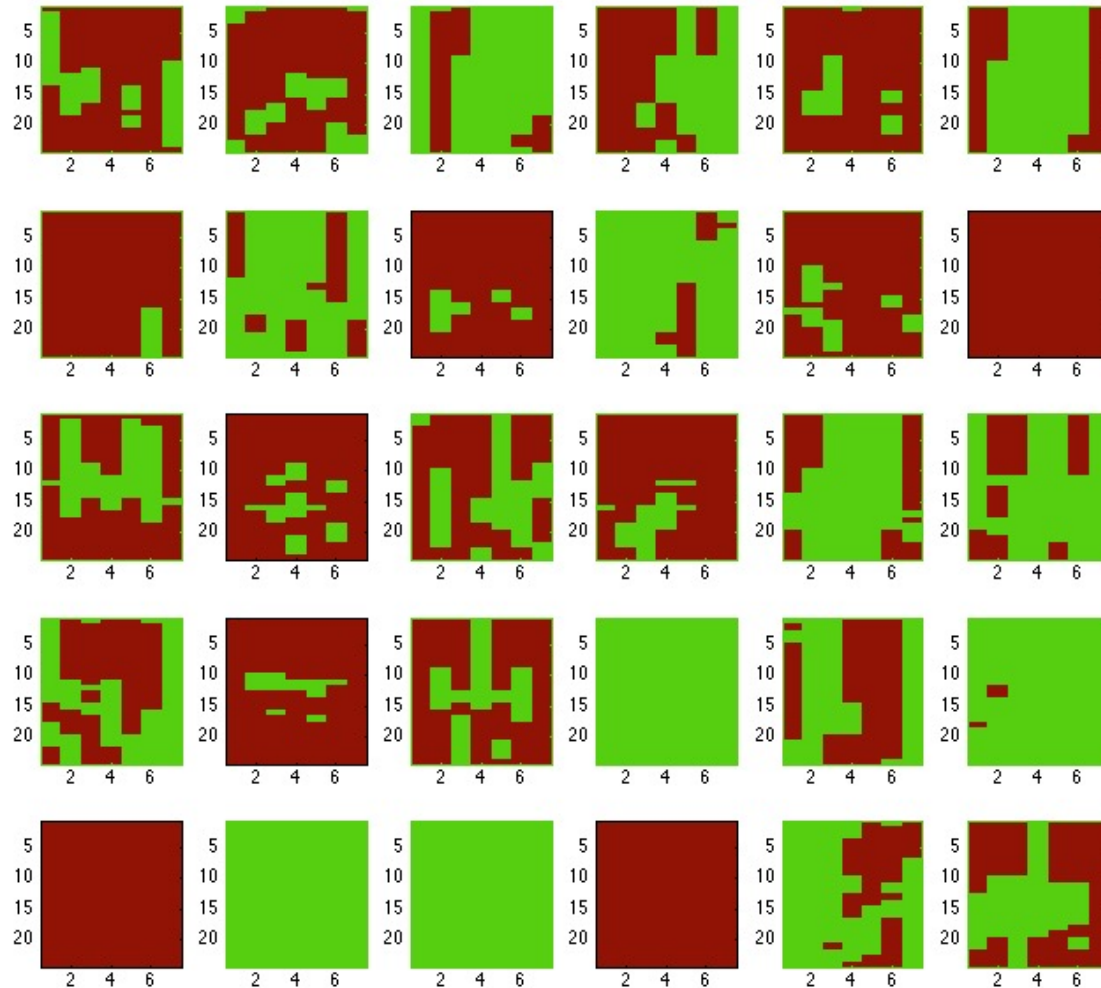
# Could Default Policies/Personas Help?

---

Ramprasad Ravichandran, Michael Benisch, Patrick Gage Kelley, and Norman M. Sadeh. [Capturing Social Networking Privacy Preferences: Can Default Policies Help Alleviate Tradeoffs between Expressiveness and User Burden?](#) *PETS '09*.

# Can You Spot a Good Default Policy?

---

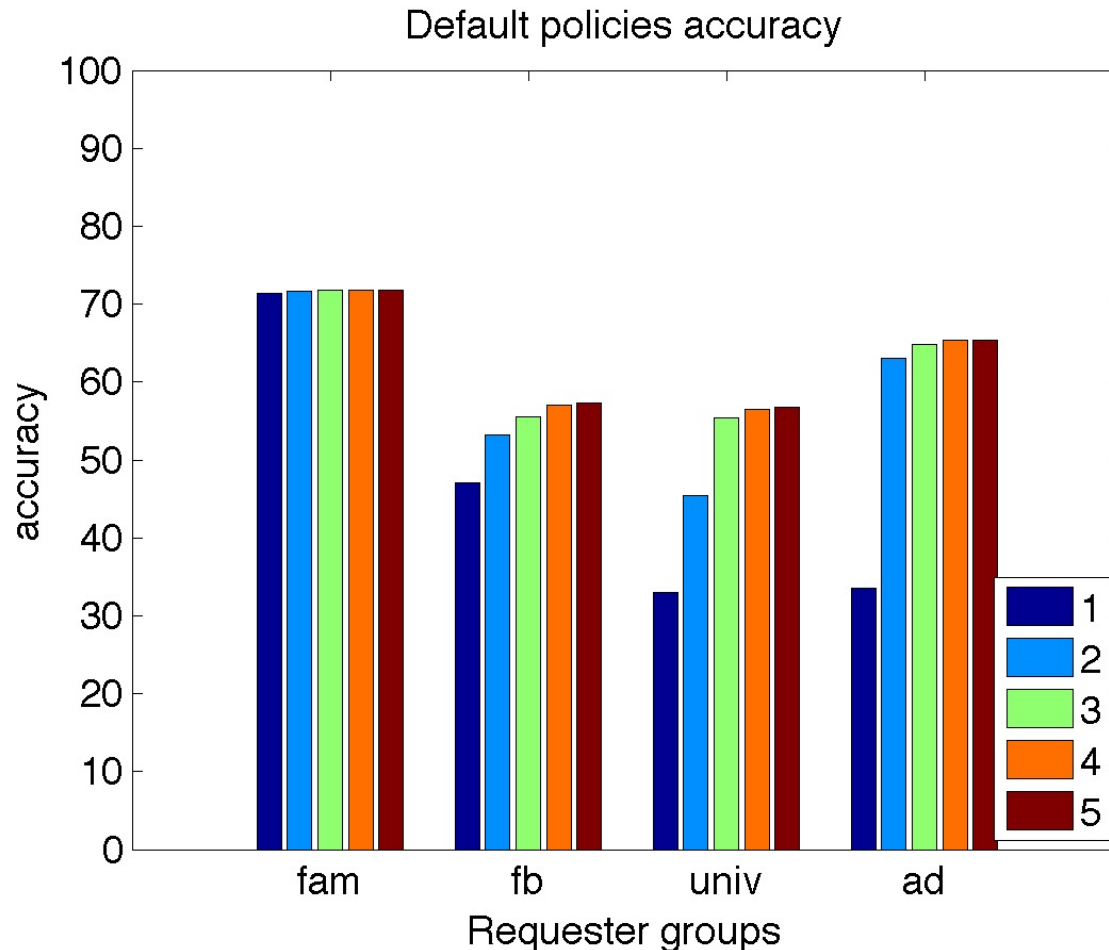


**Green: Share**  
**Red: Don't**

(each square  
represents a  
different user)

# Introducing Privacy Personas

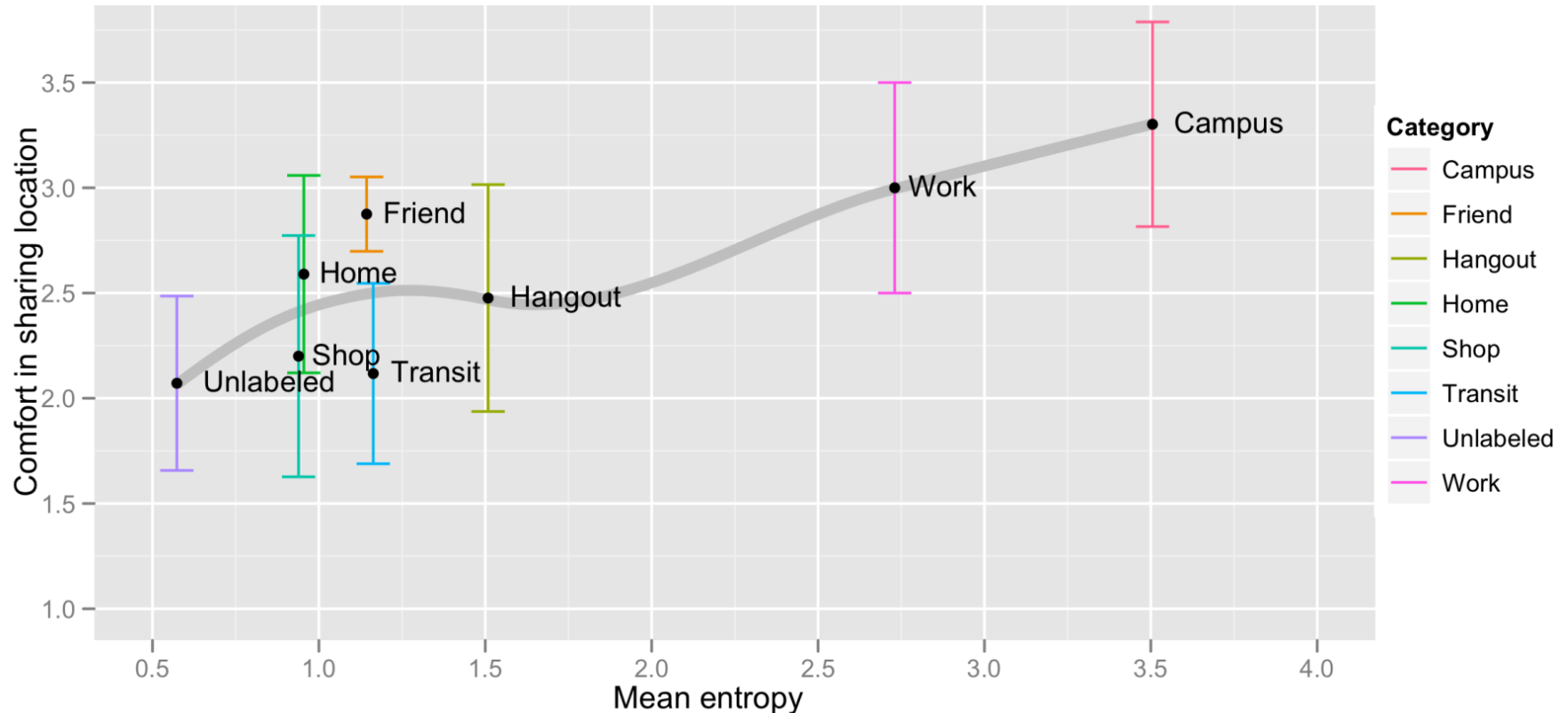
- Generating small numbers of **user-understandable privacy profiles** (“personas”)



Using canonical concepts such as “work”, “home”, “weekday”, “work-hours”

**Varying the number of personas presented to users**

# Do Locations Have Intrinsic Privacy Preferences?



## Location entropy as a possible predictor

E. Toch, J. Cranshaw, P.H. Drielsma, J. Y. Tsai, P. G. Kelley, L. Cranor, J. Hong, N. Sadeh, **"Empirical Models of Privacy in Location Sharing"**, in Proceedings of the Twelfth International Conference on Ubiquitous Computing. Ubicomp 2010

# Can We Entice Users to Tweak their Policies?

---

Janice Tsai, Patrick Kelley, Paul Hanks Drielsma, Lorrie Cranor, Jason Hong, and Norman Sadeh.

**Who's Viewed You? The Impact of Feedback in a Mobile-location System.** *CHI '09.*

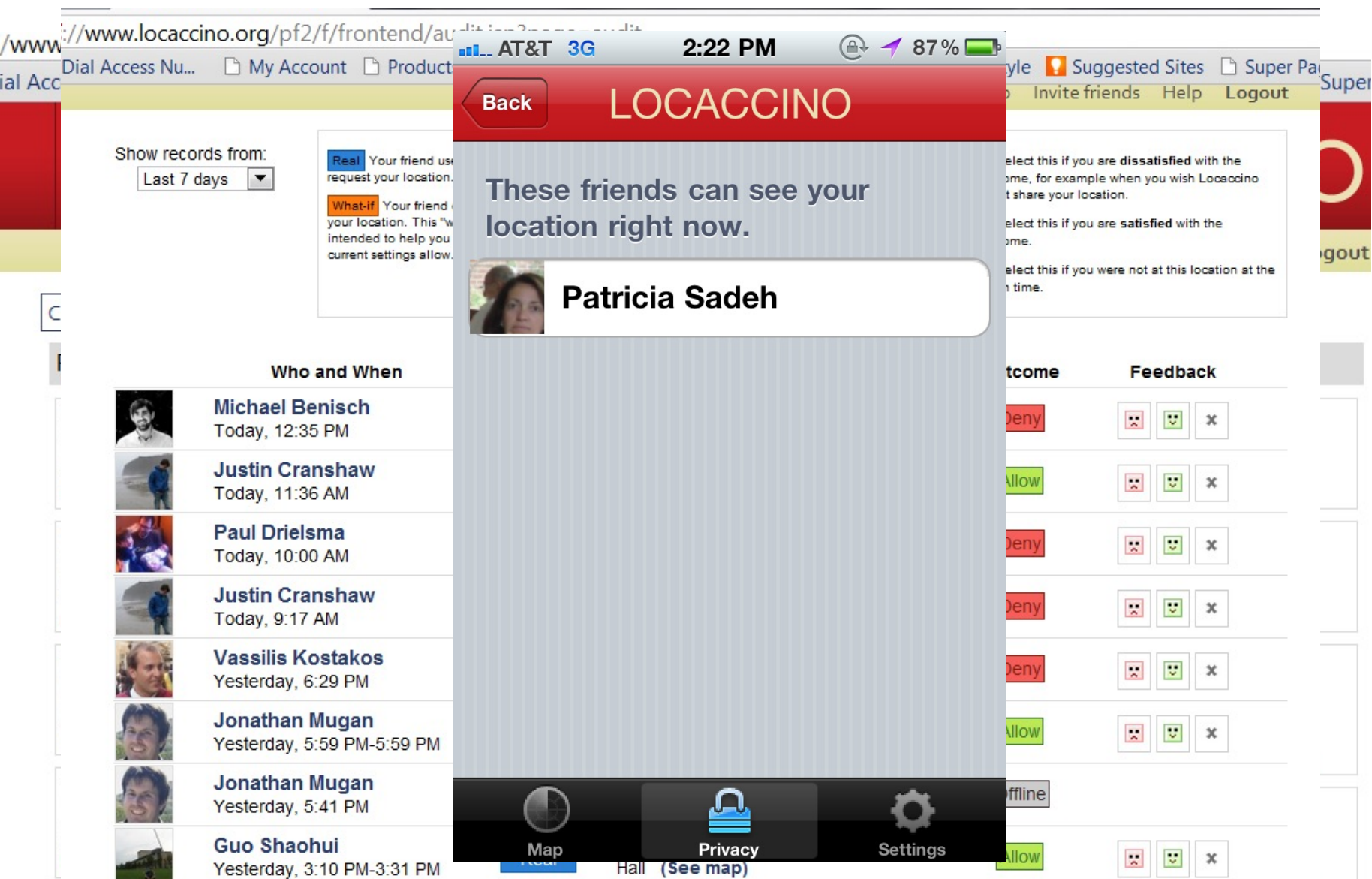
# Could Auditing Help?

---

- ❑ Users **do not always know their own policies**
- ❑ Users do not fully **understand how their rules will operate** in practice
- ❑ **Auditing ('feedback')** functionality may help users better understand the behaviors their policies give rise to



# Locaccino's Auditing Functionality

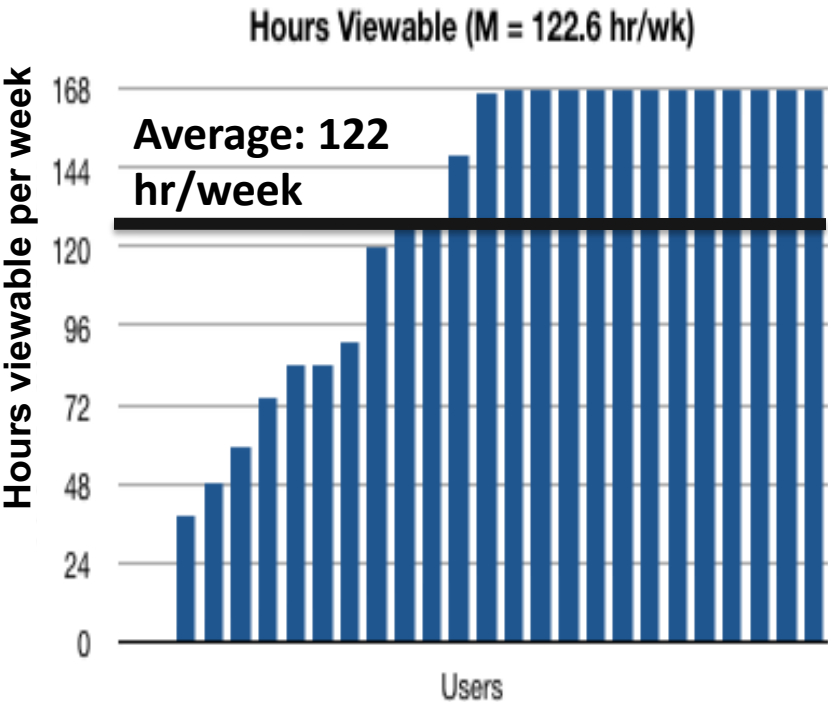


# Benefits of Auditing Functionality

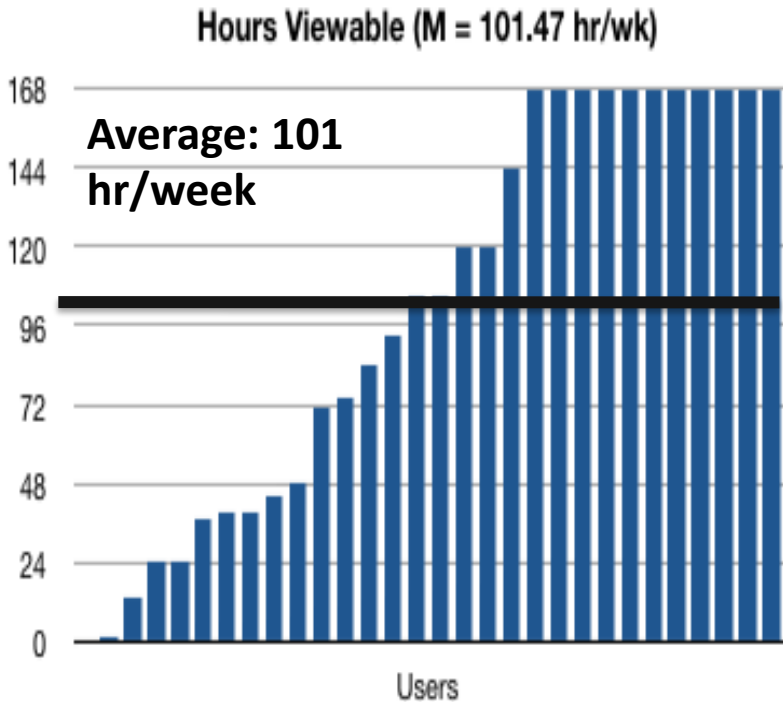
---

Examining Users' Privacy Rules **at the end** of the study

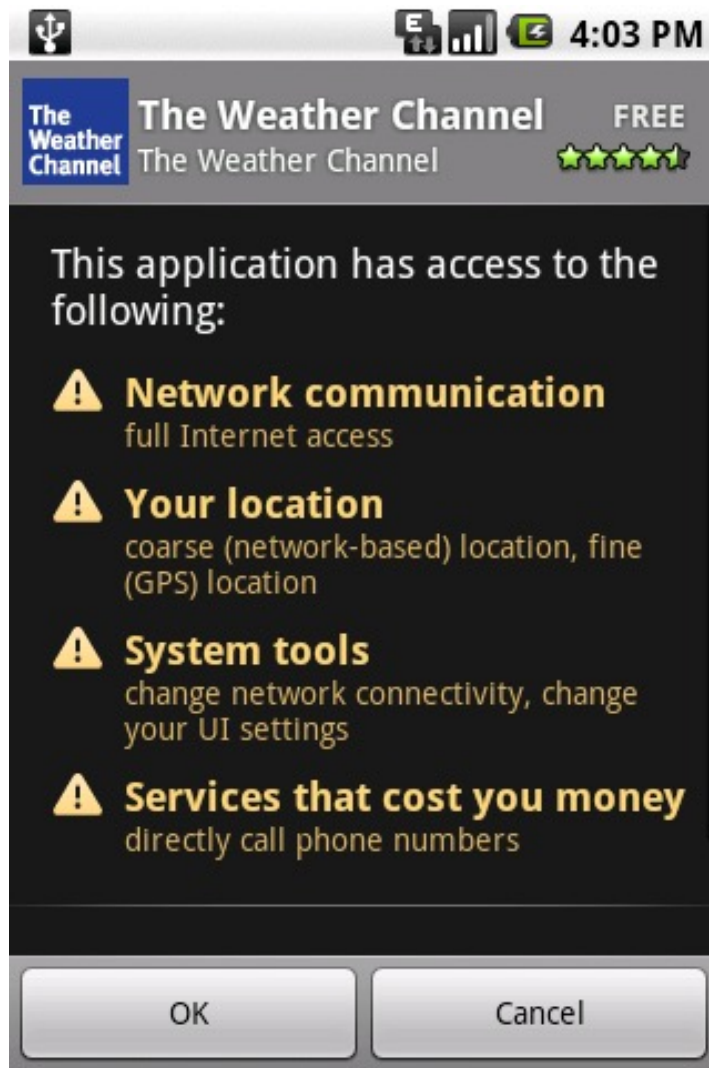
**Auditing**



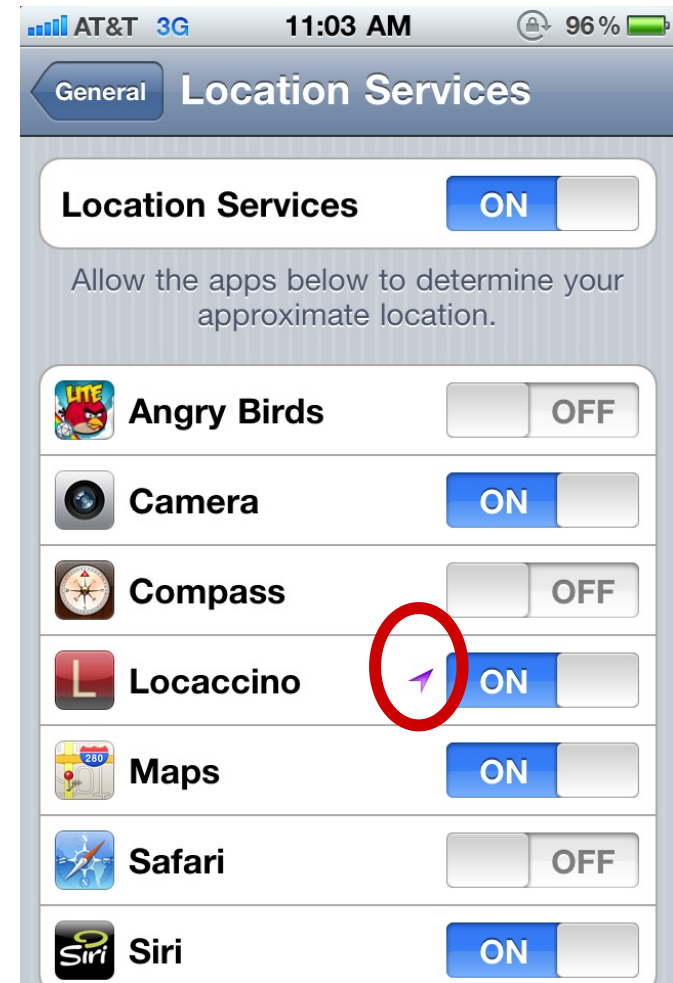
**No Auditing**



# Contrast this with Android or the iPhone



Users expected to agree upfront



Coarse 24-hour audit

# Can Machine Learning Help?

---

# User-Controllable Policy Learning (patent pending)

---

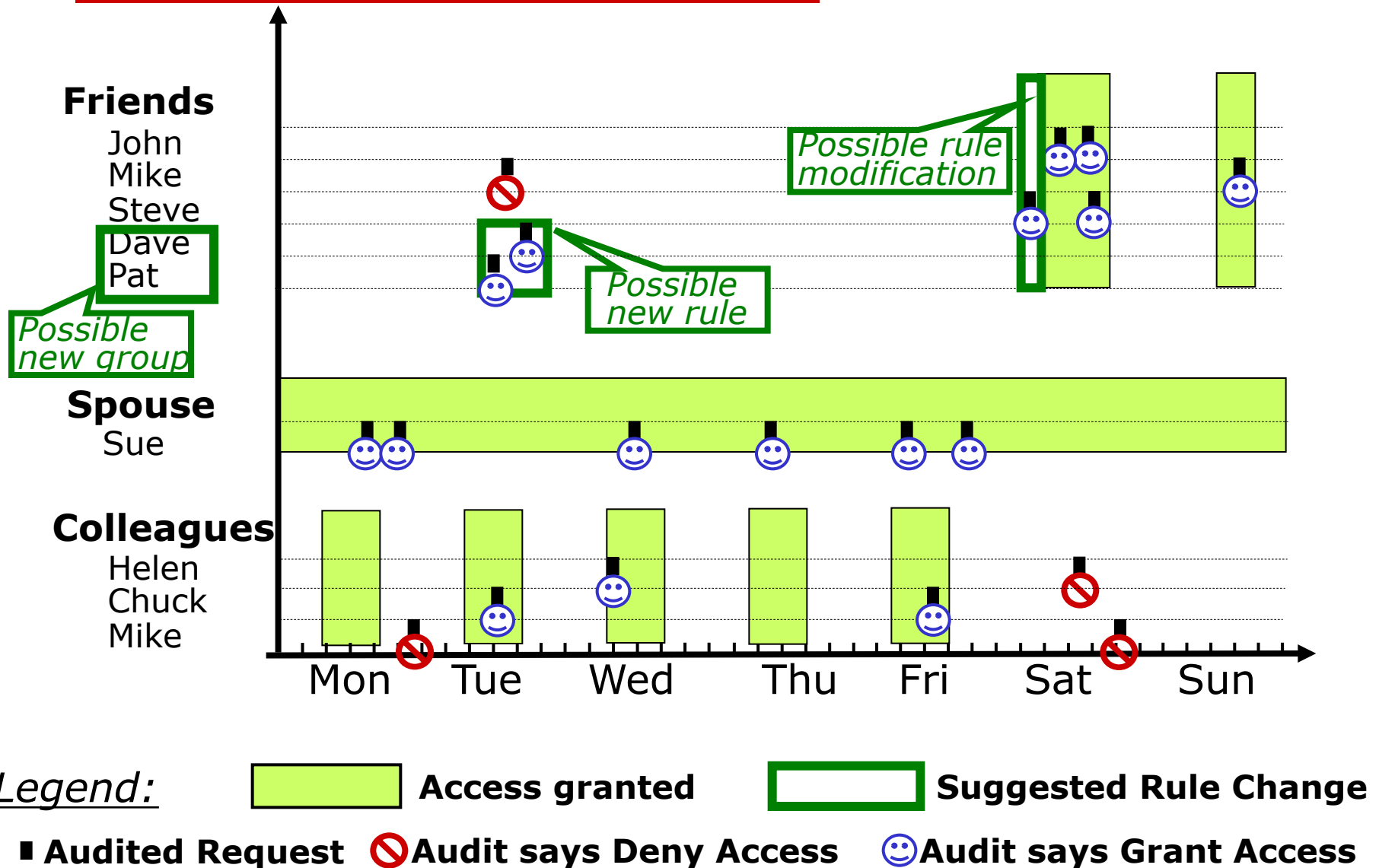
- ❑ Learning traditionally configured as a “black box” technology
- ❑ Users are unlikely to understand the policies they end up with
  - **Major source of vulnerability**
- ❑ Can we develop technology that incrementally suggests policy changes to users?
  - Tradeoff between rapid convergence and **maintaining policies that users can relate to**

Patrick Kelley, Paul Hankes Drielsma, Norman Sadeh, Lorrie Cranor. [User Controllable Learning of Security and Privacy Policies](#). *First ACM Workshop on AISec (AISec'08), ACM CCS 2008 Conference*.

J. Cranshaw, J. Mugan, and N. Sadeh. **User-Controllable Learning of Location Privacy Policies with Gaussian Mixture Models**. *Proceedings of the Twenty-Fifth Conference on Artificial Intelligence (AAAI-11)*, San Francisco, CA, August 2011.

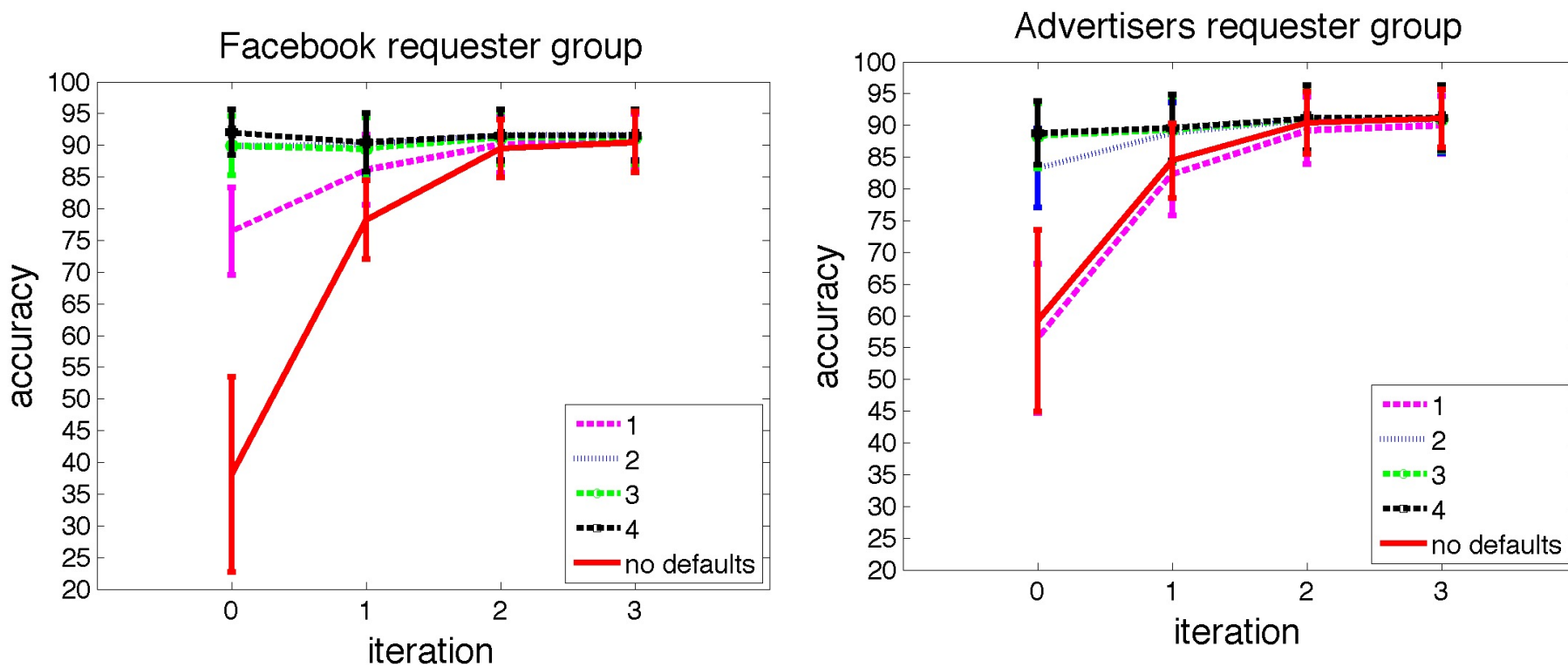
J. Mugan, T. Sharma, N. Sadeh, **Understandable Learning of Privacy Preferences Through Default Personas and Suggestions**, Carnegie Mellon Tech Report CMU-ISR-11-112, 2011 (under revision)

# Suggesting Rule Modifications based on User Feedback (patent pending)



# Default Privacy Personas & Suggestions

- Default policies and suggestions can help users make the most of rich settings



# This was just for location...

---

- ❑ **How can we scale this to other contextual attributes and more general privacy policies?**
- ❑ ...on smart phones
- ❑ ...with impatient & often distracted users
- ❑ ...who are interacting with an ever increasing number of apps and services?



# **Long-Term Vision: Personalized Privacy Assistants**

- Capable of **semi-automatically making a number of decisions** on behalf of the user
  - Too many decisions otherwise
  - Selectively asks users questions & learns
- Capable of entertaining **dialogues** to help users understand available options and make better decisions
- Capable of **nudging users** towards safer practices

# How Would this Work?

---

- ❑ Dialogues to identify relevant privacy personas
- ❑ Dialogues to evaluate privacy policies
  - Highlight departures from one's persona
- ❑ Dialogues to help configure settings
  - Leverage personas & refined preference models
  - Selectively confirm key decisions
- ❑ Dialogues to refine preference models
- ❑ Auditing dialogues & even nudging
  - *"Did you know that since you installed this app two days ago, ...."*

---

# **Is User-Controllable Privacy an Oxymoron?**

# Concluding Remarks

---

- ❑ Privacy is really complex
- ❑ Usable privacy is even more complex
- ❑ **Short-term:**
  - Expose a limited number of simple decisions
  - Auditing
- ❑ **Medium-term:** User-oriented machine learning
- ❑ **Longer-term:** towards personalized privacy assistants
- ❑ ...May need some help from lawmakers and regulators too

---

# Q&A



# Acknowledgements

---

- ❑ Research funded by the US National Science Foundation, the US Army Research Office, Google, CMU CyLab, Google, Nokia, FranceTelecom, ICTI, Microsoft, Pitney Bowes.

# References - I

---

- ❑ M. Benisch, P.G. Kelley, N. Sadeh, and L.F. Cranor, "Capturing Location-Privacy Preferences: Quantifying Accuracy and User-Burden Tradeoffs", *Journal of Personal and Ubiquitous Computing*. Volume 15 Issue 7, October 2011 (published online December 7, 2010).
- ❑ J. Tsai, P.G. Kelley, L.F. Cranor and N.M. Sadeh, "Location Sharing Technologies: Privacy Risks and Controls", *I/S: A Journal of Law and Policy for the Information Society*, Vol. 6, No. 2, Summer 2010, pp. 119-151.
- ❑ N. Sadeh, J. Hong, L. Cranor, I. Fette, P. Kelley, M. Prabaker, and J. Rao, "Understanding and Capturing People's Privacy Policies in a Mobile Social Networking Application", *Journal of Personal and Ubiquitous Computing*, Vol. 13, No. 6, August 2009.
- ❑ Gandon, F. and Sadeh, N., "Semantic Web Technologies to Reconcile Privacy and Context Awareness", *Journal of Web Semantics*. Vol. 1, No. 3, 2004
- ❑ P. Gage Kelley, S. Consolvo, L. Cranor, J. Jung, N. Sadeh, D. Wetherall, "A Conundrum of Permissions: Installing Applications on an Android Smartphone", Proc. Of Workshop on Usable Security (USEC2012), collocated with the 16<sup>th</sup> International Conference on Financial Cryptography and Data Security, March 2012

# References - II

---

- Justin Cranshaw, Jonathan Mugan, Norman Sadeh, "User-Controllable Learning of Location Privacy Policies with Gaussian Mixture Models", Proceedings of the 25<sup>th</sup> AAAI Conference on Artificial Intelligence, AAAI-11, August 2011.
- Patrick Gage Kelley, Lorrie Cranor, Norman Sadeh, "An Investigation into Facebook Friends Grouping", Proceedings of the 13<sup>th</sup> IFIP Conference on Human Computer Interaction (INTERACT), September 2011
- P. Gage Kelley, M. Benisch, L. Cranor and N. Sadeh, "When Are Users Comfortable Sharing Locations with Advertisers", in Proceedings of the 29<sup>th</sup> annual SIGCHI Conference on Human Factors in Computing Systems, CHI2011, May 2011. Also available as CMU School of Computer Science Technical Report, CMU-ISR-10-126 and CMU CyLab Tech Report CMU-CyLab-10-017.
- R. Balebako, P.G. Leon, J. Mugan, A. Acquisti, L.F. Cranor, N. Sadeh, "Nudging Users Towards Privacy on Mobile Devices", CHI 2011 workshop article, May 2011
- J. Cranshaw, E. Toch, J. Hong, A. Kittur, N. Sadeh, "Bridging the Gap Between Physical Location and Online Social Networks", in Proceedings of the Twelfth International Conference on Ubiquitous Computing. Ubicomp 2010
- E. Toch, J. Cranshaw, P.H. Drielsma, J. Y. Tsai, P. G. Kelley, L. Cranor, J. Hong, N. Sadeh, "Empirical Models of Privacy in Location Sharing", in Proceedings of the Twelfth International Conference on Ubiquitous Computing. Ubicomp 2010



# References - III

---

- ❑ Jialiu Lin, Guang Xiang, Jason I. Hong, and Norman Sadeh, "Modeling People's Place Naming Preferences in Location Sharing", Proc. of the 12th ACM International Conference on Ubiquitous Computing, Copenhagen, Denmark, Sept 26-29, 2010.
- ❑ Karen Tang, Jialiu Lin, Jason Hong, Norman Sadeh, Rethinking Location Sharing: Exploring the Implications of Socially-Driven vs. Purpose-Driven Location Sharing. Proc. of the 12th ACM International Conference on Ubiquitous Computing, Copenhagen, Denmark, Sept 26-29, 2010.
- ❑ R. Ravichandran, M. Benisch, P. G. Kelley, and N. Sadeh, "Capturing Social Networking Privacy Preferences: Can Default Policies Help Alleviate Tradeoffs between Expressiveness and User Burden?", Proceedings of the 2009 Privacy Enhancing Technologies Symposium, August 2009.
- ❑ J. Tsai, P. Kelley, P. Hanks Drielsma, L. Cranor, J. Hong, N. Sadeh "Who's Viewed You? The Impact of Feedback in a Mobile Location Applications", in Proceedings of the 27<sup>th</sup> annual SIGCHI Conference on Human Factors in Computing Systems (CHI 2009), April 2009.
- ❑ P.G. Kelley, P. Hanks Drielsma, N. Sadeh, and L.F. Cranor, "User-Controllable Learning of Security and Privacy Policies", First ACM Workshop on AISEc (AISEc'08), ACM CCS 2008 Conference. Oct. 2008
- ❑ J. Cornwell, I. Fette, G. Hsieh, M. Prabaker, J. Rao, K. Tang, K. Vaniea, L. Bauer, L. Cranor, J. Hong, B. McLaren, M. Reiter, N. Sadeh, "User-Controllable Security and Privacy for Pervasive Computing". Proceedings of the 8<sup>th</sup> IEEE Workshop on Mobile Computing Systems and Applications ("HotMobile 2007"). Feb. 2007.