Mobile Location Privacy:
Forces at Play, Attitudes and Challenges

Norman M. Sadeh
Professor, School of Computer Science
Director, Mobile Commerce Lab.
Carnegie Mellon University
www.cs.cmu.edu/~sadeh

Outline

- Context and Trends
- People's attitudes
- Are there cultural differences?
- Why is this a challenging area …or are we doomed to fail?
- Possible paths forward
- Location privacy: A harbinger of future privacy debates

Context & Trends

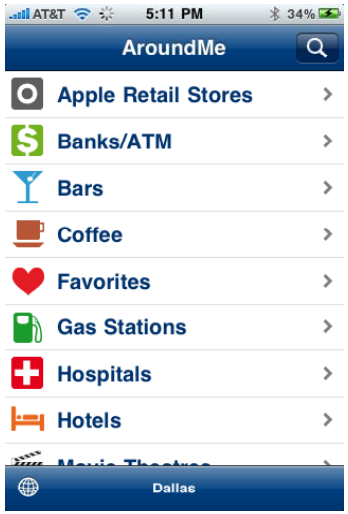
Everyone has at least one mobile phone

- Over 5 billion cell phone users today
- This year: 1.3 billion cell phones will be sold
  - Including **500 million smart phones**
- Hong Kong: one of the highest penetration rates in the world: **192%**

Location Tracking

- **Price of GPS chipsets has dropped under 2 US dollars**
  - 295M GPS-enabled handsets sold in 2010.
  - 940M expected to be sold in 2015
- 1 billion cell phones are also **WiFi**-enabled
- Extended battery life & new hybrid location sensing: **continuous fine-grained location tracking** now possible (beyond cell triangulation)
- Not just your cell phone: cameras, toll collection, swipe cards, laptops, etc.

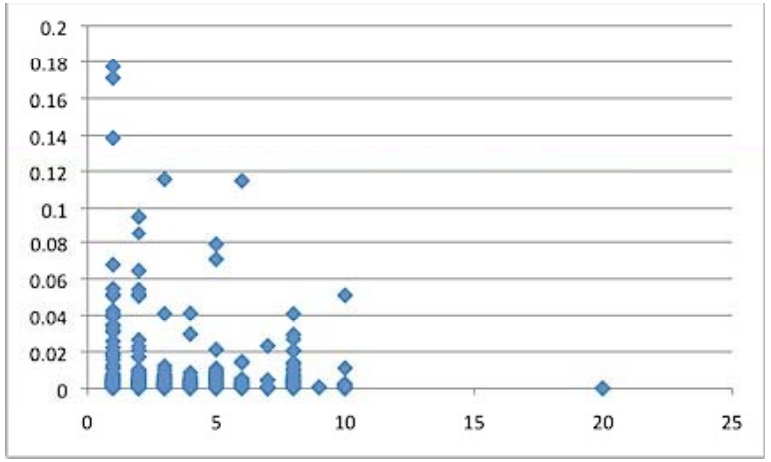
A Powerful Contextual Attribute



Location-Based Apps

- 24% of US adults use apps (Nielsen Sept 2010)
- Hundreds of thousands of mobile apps
  - Including **10,000's of location-based apps**

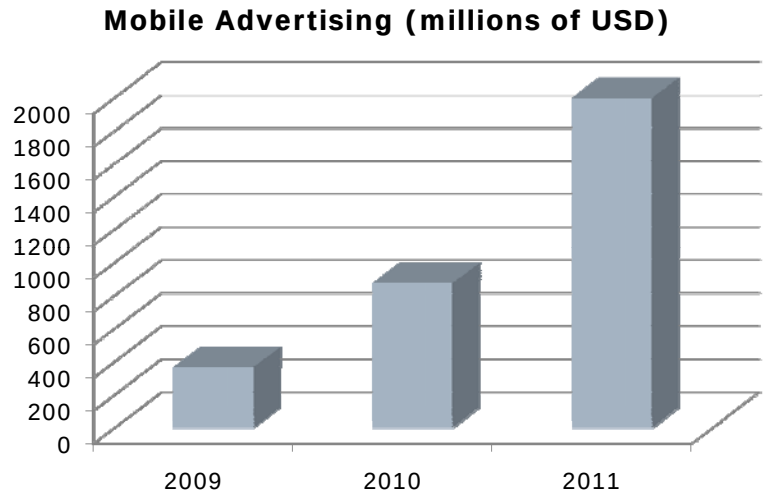
Game Apps: Popularity vs. Price



http://mobileorchard.com/price-and-popularity-the-iphone-app-stores-data-shows-whos-making-the-big-money/

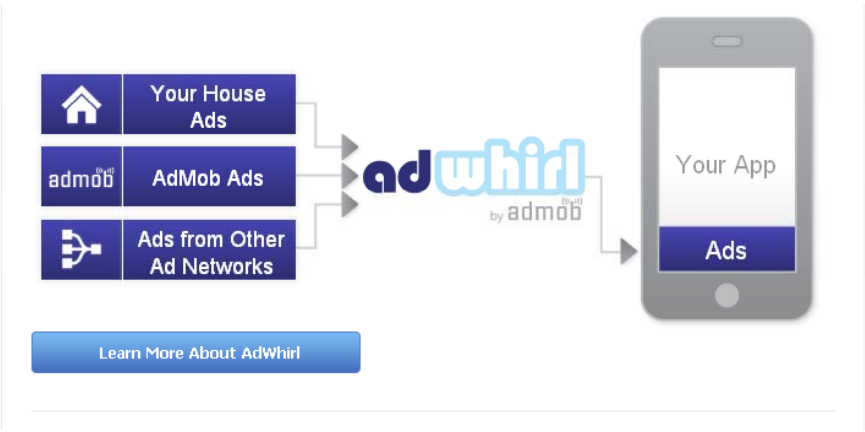
HOW DO THESE CHEAP APPS PAY FOR THEMSELVES?

Mobile Advertising (US Only)



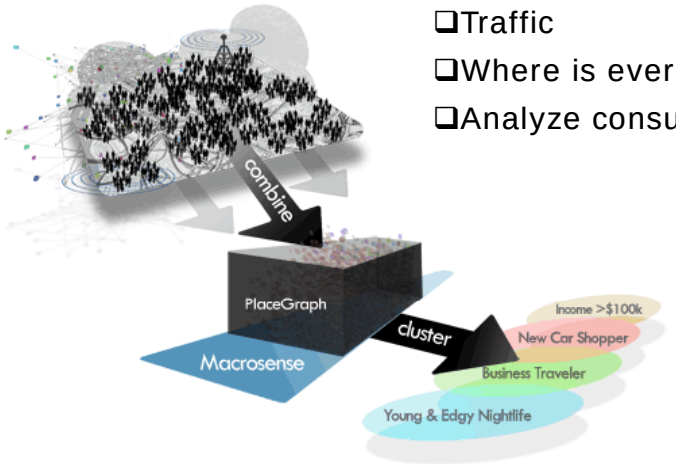
Source: IDC December 2010 --- worldwide: multiply by 2 (Gartner)

In-App Advertising



Cell phones as Sensor Nets

- ❑Traffic
- ❑Where is everyone right now?
- ❑Analyze consumer behavior



Source: Sense Networks

Location Privacy

"...the ability of an individual to move in public space with the expectation that under normal circumstances their location will not be systematically and secretly recorded for later use"

(*Electronic Frontier Foundation*)

Tracking Your Location

...would enable someone to answer **questions such as:**

- Did you go to an anti-war rally on Tuesday?
- Did you walk into an abortion clinic?
- Have you been checking into a motel at lunchtimes?
- Were you the person who anonymously tipped off safety regulators about the rusty machines?
- Which church do you attend?
- Who is my ex-girlfriend going to dinner with?

(source: EFF)

Wall Street Journal Study (Dec. 2010)

Study of 101 Apps (iPhone and Android):

- 56 are sharing unique device ID with other companies without user consent
- 47 share user's location

THE WALL STREET JOURNAL.
WSJ.com

WHAT THEY KNOW | DECEMBER 18, 2010

Your Apps Are Watching You

A WSJ Investigation finds that iPhone and Android apps are breaching the privacy of smartphone users

By SCOTT THURM and YUKARI IWATANI KANE

iPhone Fiasco


'20/2011 iPhone keeps record of everywhere you...

guardian.co.uk

iPhone keeps record of everywhere you go

Privacy fears raised as researchers reveal file on iPhone that stores location coordinates and timestamps of owner's movements

Charles Arthur
guardian.co.uk, Wednesday 20 April 2011 14.06 BST

- **Unencrypted file recording up to a year of location data**
- Google & Microsoft collect location data too

…In short, everyone seems to be misbehaving…

Multiple Facets to the Problem

- Location being used to support meaningful functionality
- Location being retained longer than needed
- Location being used for other purposes – including sharing, data mining, etc.
- Location being collected/used without user's knowledge and/or consent
  - **Are systems optimally designed?**
  - **Are practices adequately disclosed?**
  - **Are users given viable options?**

Attitudes Towards Location Privacy

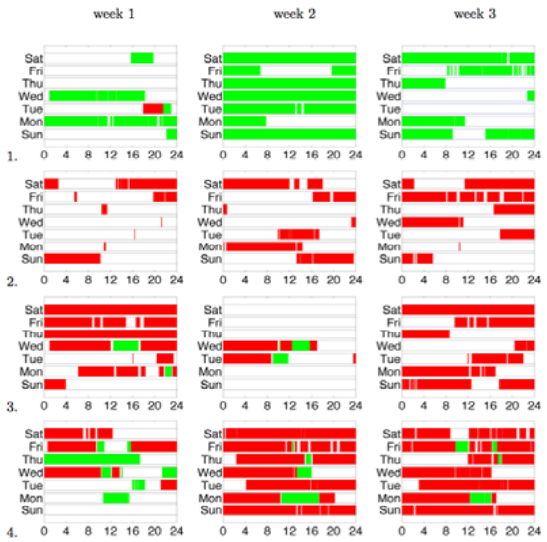
How Do People Feel?

- Pew Research Center's Internet & American Life Project: **Only 4 percent of Americans online have used location sharing such as Foursquare**
  - Survey of 3,000 adults in Aug-Sept 2010
- TRUSTe Q1 2011 survey of 1,000 mobile users: **38% report privacy is their number one concern** when using mobile apps
  - Ahead of all other concerns

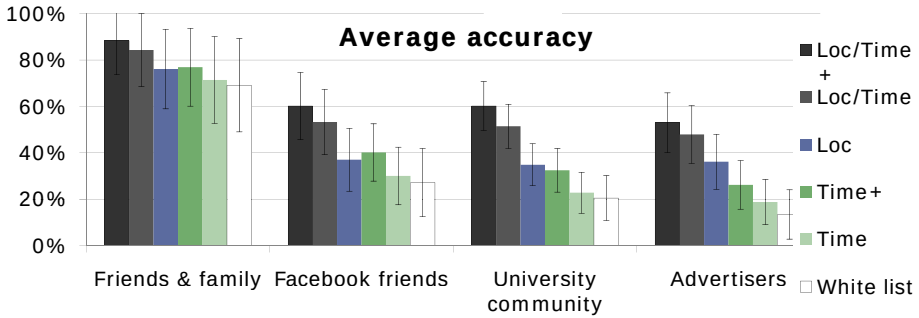
Location Sharing with Peers & Advertisers

People have **diverse location privacy Preferences**

Example of 4 users over 3 weeks: willingness to disclose their location to colleagues

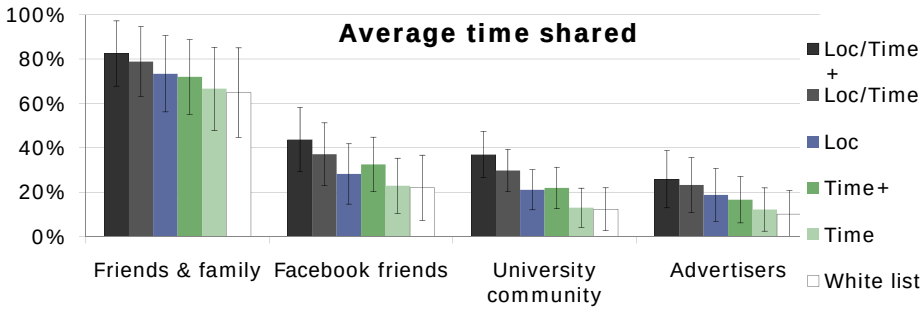


…Rich Preferences…



Loopt & Latitude: Failure due to **conservative defaults & restrictive settings** ("white lists")

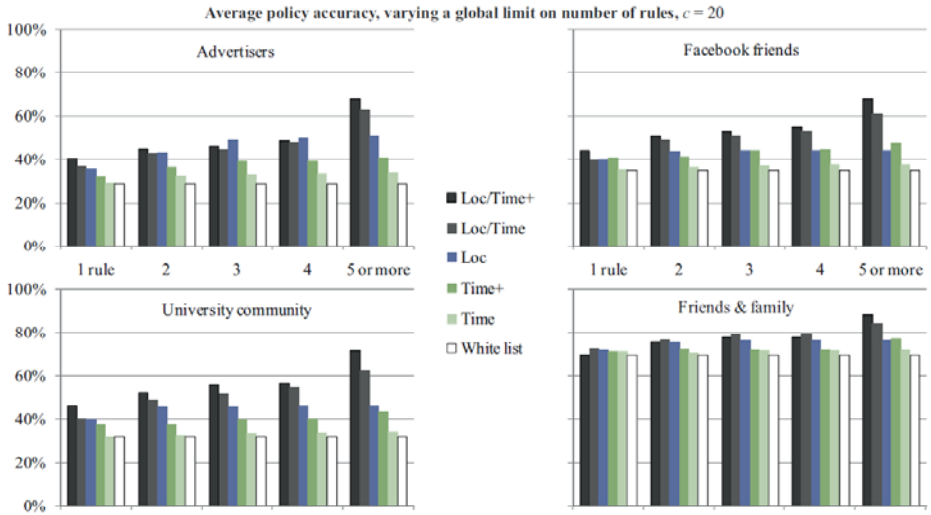
Here's the Real Kicker!



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



Are There Cultural Differences?

Are There Cultural Differences?

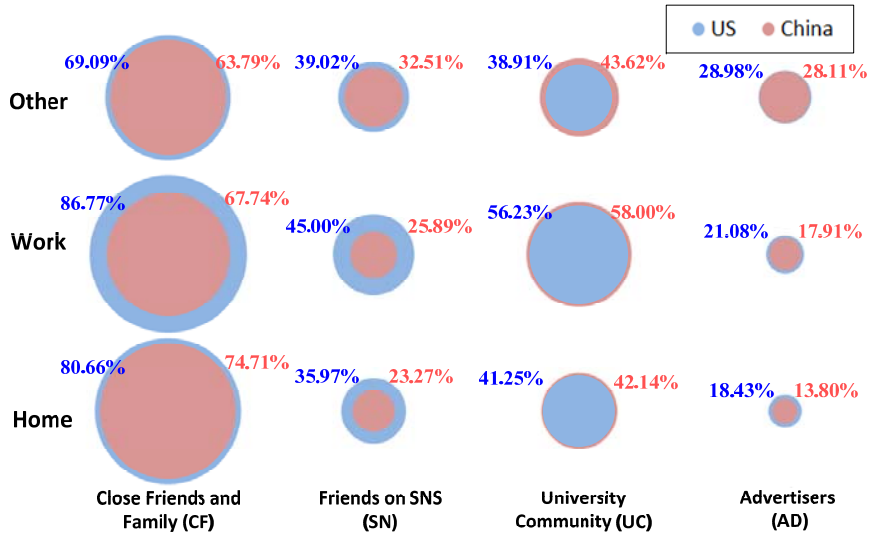
- US-China study (Dec. 2010-Feb. 2011)
- 29 users in the US and 30 users in China
- Similar demographics
- Tracked for a total of about 19,000 hours
- Collected & analyzed location sharing preferences

Willingness to Disclose Fine Grain Location

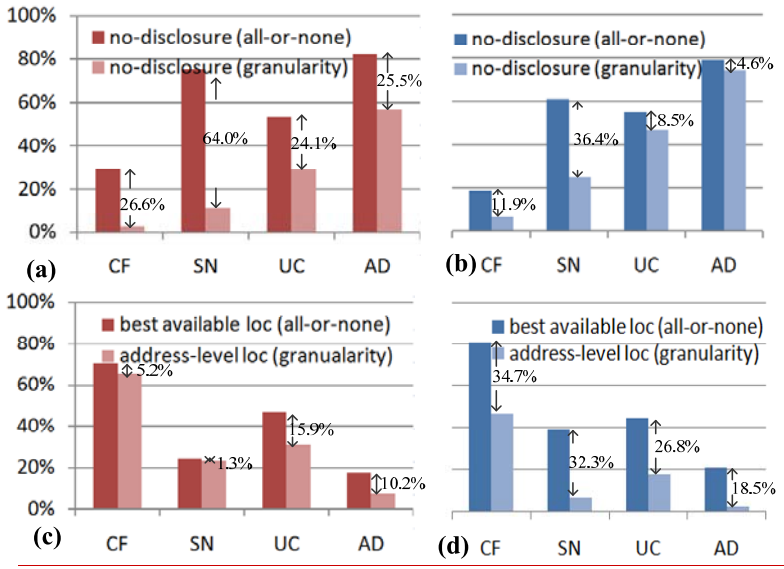
	China	U.S.	P value
Close Friends & Family (CF)	70.63%	81.46%	<0.05
Friends on SNS (SN)	24.53%	39.05%	<0.05
University Community (UC)	46.87%	44.54%	0.13
Advertisers (AD)	17.61%	21.06%	<0.1

By and large, privacy preferences are fairly similar
Chinese participants seemed a little more conservative, except when it comes to sharing with members of the university community

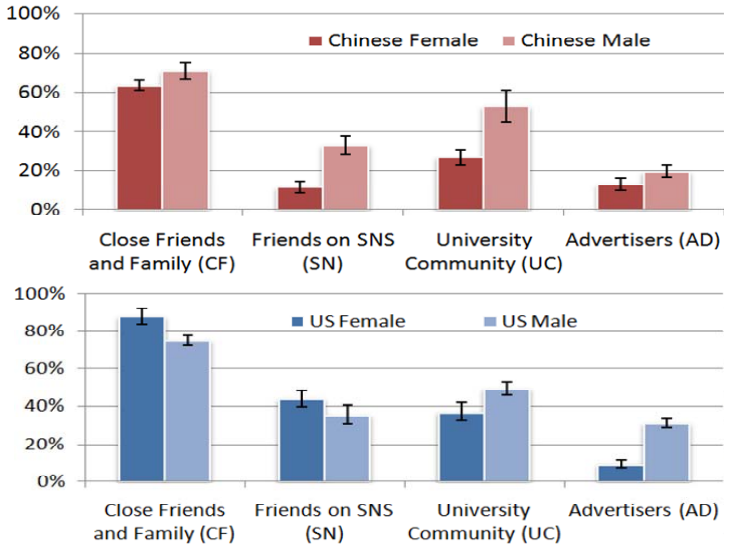
Biggest Differences: Sharing with SN Friends and when at work



Modulating the Granularity of Disclosures



Gender Differences

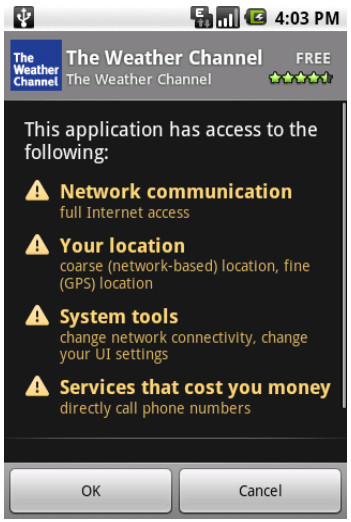


Implications

- **Most people seem to value their location privacy** and are not willing to share indiscriminately
- Users in both the US and China seem to require **rich settings**
- Default settings and early adopters may however be different
- Further research is required: Study limited to members of university communities

Why Is This Challenging…or Are We Doomed to Fail?

Inadequate Disclosures and Settings



Users expected to agree upfront

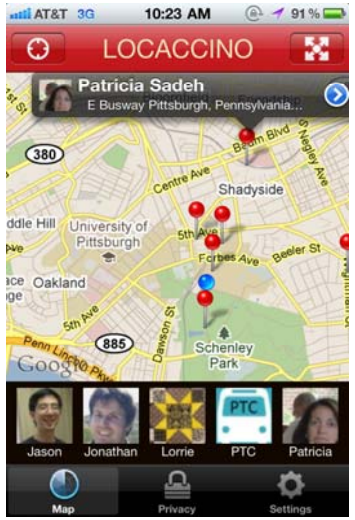
Coarse 24-hour audit

But More Complex Settings Can Fail Too..

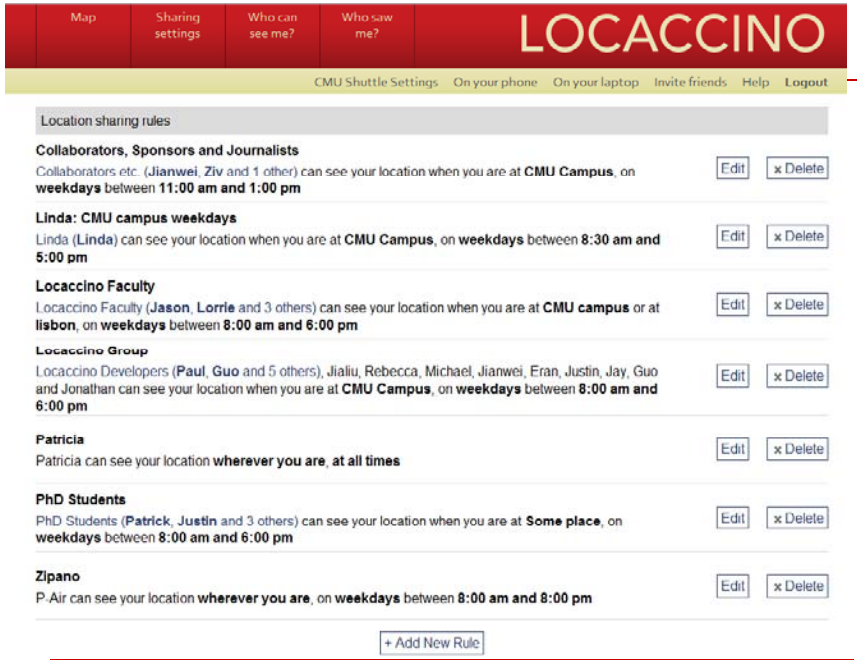
How Can We Help Users Make the Most of Richer Settings?

Experimenting with Our Own Location Sharing App

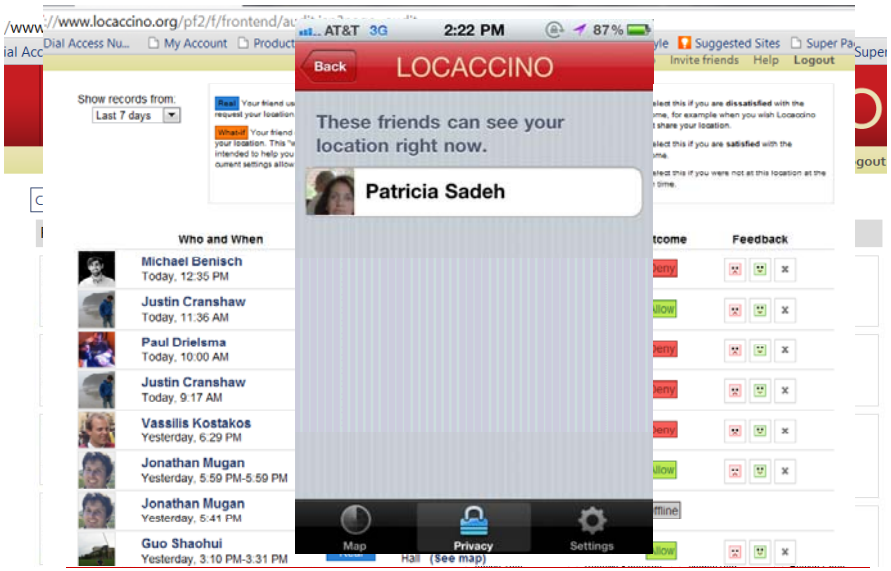
- **More expressive privacy settings**
  - "My colleagues can only see my location when I'm on campus and only weekdays 9am-5pm"
  - **Invisible button**
- **Auditing functionality**
- Available on Android Market, iPhone client, Ovi, laptop clients
- Tens of thousands of downloads over the past year



www.locaccino.org

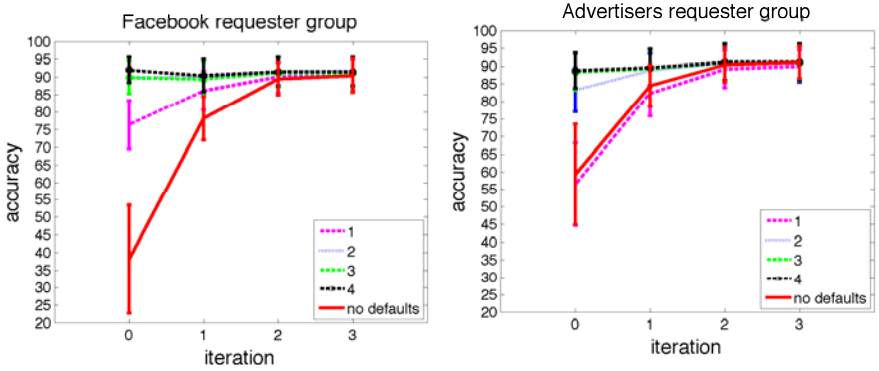


Auditing & Feedback Make a Huge Difference

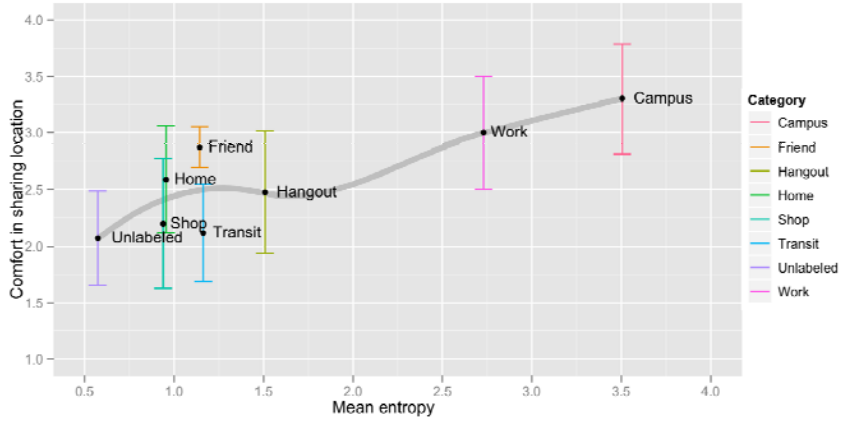


Default Privacy Personas & Suggestions

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



Do Locations Have Intrinsic Privacy Preferences?



Location entropy as a possible predictor

Education & Nudging

Making up for fundamental human cognitive biases

Multiple Paths Forward

- **Cryptographic protocols**
  - ..and generally protocols that disclose less information
- **Minimize collection and retention**
  - **At design time**
  - Data sanitization
- **Disclose practices and give meaningful choices**
  - **Move towards new UI technologies**
- **Strengthen legal and regulatory framework**
  - Striking a balance between economic forces & people's privacy expectations – **"Devil's in the details"**
- **Educate** people about potential risks, incl. **"nudges"**

Harbinger of Future Privacy Debates

Location is just one of many sensitive contextual attributes/piece of PII

Q&A

mobile commerce lab

Relevant Websites

- *www.mcom.cs.cmu.edu/*
- www.locaccino.com
- http://mcom.cs.cmu.edu/user-controllable-security-and-privacy/
- www.eff.org

Relevant Publications - I

- Norman Sadeh, "M-Commerce: Technologies, Services and Business Models", Wiley 2002
- Norman Sadeh, Jason Hong, Lorrie Cranor, Ian Fette, Patrick Kelley, Madhu Prabaker, and Jinghai Rao. Understanding and Capturing People's Privacy Policies in a Mobile Social Networking Application *Journal of Personal and Ubiquitous Computing 2009.*
- 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.*
- Patrick Kelley, Paul Hankes Drielsma, Norman Sadeh, Lorrie Cranor. User Controllable Learning of Security and Privacy Policies. *AISec 2008.*
- Michael Benisch, Patrick Gage Kelley, Norman Sadeh, Lorrie Faith Cranor. Capturing Location Privacy Preferences: Quantifying Accuracy and User Burden Tradeoffs. CMU-ISR Tech Report 10-105, March 2010. Accepted for publication in *Journal of Personal and Ubiquitous Computing*
- Janice Tsai, Patrick Kelley, Paul Hankes Drielsma, Lorrie Cranor, Jason Hong, and Norman Sadeh. Who's Viewed You? The Impact of Feedback in a Mobile-location System. *CHI '09.*
- Jason Cornwell, Ian Fette, Gary Hsieh, Madhu Prabaker, Jinghai Rao, Karen Tang, Kami Vaniea, Lujo Bauer, Lorrie Cranor, Jason Hong, Bruce McLaren, Mike Reiter, and Norman Sadeh. User-Controllable Security and Privacy for Pervasive Computing. *The 8th IEEE Workshop on Mobile Computing Systems and Applications (HotMobile 2007).* 2007.
- Norman Sadeh, Fabien Gandon and Oh Buyng Kwon. Ambient Intelligence: The MyCampus Experience School of Computer Science, Carnegie Mellon University, Technical Report CMU-ISRI-05-123, July 2005.

Relevant Publications - II

- P. Gage Kelley, M. Benisch, L. Cranor and N. Sadeh, "When Are Users Comfortable Sharing Locations with Advertisers", in Proceedings of the 29th 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.
- 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
- 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 Social-Driven vs. Purpose-Driven Location Sharing. Proc. of the 12th ACM International Conference on Ubiquitous Computing, Copenhagen, Denmark, Sept 26-29, 2010.

Acknowledgements

- Research funded by the US National Science Foundation, the US Army Research Office, CMU CyLab, Microsoft, Google, Nokia, FranceTelecom, and ICTI

mobile commerce lab

Background Slides

Concept of Privacy

- Moral right of individuals to be left alone, free from surveillance or interference from other individuals or organizations, including state
  - There are obviously conflicting considerations
    - e.g. security and safety
- Legal Protection: founding documents of many countries

Information Privacy

- The claim that *certain information should not be collected by government or businesses – or possibly only under special circumstances* and subject to various rules
  - e.g. individuals have some control over the use of information collected about them

Hong Kong Personal Data Ordinance (Dec. 1996)

Six Principles:

1. **Purpose & Manner of Collection** has to be disclosed to data subject
2. **Accuracy and Duration of Retention** of Personal Data: data should be uptodate and only retained as long as necessary
3. **Use of Personal Data**: only for the purpose for which data was collected – unless otherwise agreed by data subject
4. **Security of Personal Data**
5. **Notification**: Open policies about data being collected & for what purpose
6. **Access to personal data**: right to review and correct data about oneself

Hong Kong Personal Data Ordinance

- Personal data can only be used for the **purpose** for which it was collected – **no frivolous collection**
  - This also restricts sharing
- Purpose has to be **stated from the beginning**
- People should have the right to inspect information held about them within 40 days of their asking
  - May involve a fee
- Data has to be **corrected if erroneous**
- Data has to be **secure**
- No direct marketing or teleselling **if someone opts out**
- Individuals can sue if damage results from the release of confidential data, or from inaccurate data or other breach
- **Note**: This is a very **approximate summary** – read the text of the Ordinance for a more detailed & accurate understanding