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.

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**

Copyright © Norman Sadeh, 2005-2011
HOW DO THESE CHEAP APPS PAY FOR THEMSELVES?

Mobile Advertising (US Only)

Mobile Advertising (millions of USD)

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)

Copyright © Norman Sadeh, 2005-2011

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)

Copyright © Norman Sadeh, 2005-2011

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

Copyright © Norman Sadeh, 2005-2011

iPhone Fiasco

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

Copyright © Norman Sadeh, 2005-2011
...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?

- 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

<table>
<thead>
<tr>
<th></th>
<th>China</th>
<th>U.S.</th>
<th>P value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Close Friends &amp; Family (CF)</td>
<td>70.63%</td>
<td>81.46%</td>
<td>&lt;0.05</td>
</tr>
<tr>
<td>Friends on SNS (SN)</td>
<td>24.53%</td>
<td>39.05%</td>
<td>&lt;0.05</td>
</tr>
<tr>
<td>University Community (UC)</td>
<td>46.87%</td>
<td>44.54%</td>
<td>0.13</td>
</tr>
<tr>
<td>Advertisers (AD)</td>
<td>17.61%</td>
<td>21.06%</td>
<td>&lt;0.1</td>
</tr>
</tbody>
</table>

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 and when at work.
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

Copyright © Norman Sadeh, 2005-2011

But More Complex Settings Can Fail Too..

Copyright © Norman Sadeh, 2005-2011

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

Copyright © Norman Sadeh, 2005-2011
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
Relevant Websites

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

Acknowledgements

Research funded by the US National Science Foundation, the US Army Research Office, CMU CyLab, Microsoft, Google, Nokia, France Telecom, and ICTI
**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 up to date 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