Privacy, Law, and Smartphones

Rebecca Balebako

Oct. 29, 2015
Agenda

• Quiz
• Reading discussion
• Permission notices on major platforms
• Policy on smartphone privacy
• Research on smartphone privacy
By the end of class....

- Understand privacy concerns around smartphones
- Understand how privacy notices on smartphones are evolving
- Identify the research questions in several smartphone privacy research projects
- Recognize several methods for addressing the research questions
Smartphones allow data sharing
Privacy and security concerns

• Immature technology
• Phones always with user and always on
• Data sharing might be unknown to user
  – Sensors (GPS location, camera, accelerometer, gyroscope)
• Inferences can be made
Permissions warnings differ on time and content

Android 2012

iOS 2012
Android Permission Manager (AppOps)

- Introduced in Android 4.3, albeit hidden by default.
  - need a launcher app.
- Made in completely inaccessible in Android 4.4.2.
- Next version of Android will have just-in-time permissions
Research questions

• Would AppOps provide any benefit to smartphone users?
• Would additional notices or nudges benefit users?
<table>
<thead>
<tr>
<th>App ops</th>
<th>LOCATION</th>
<th>PERSONAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Play services</td>
<td>wi-fi scan, cell scan, fine location, GPS, coarse location</td>
<td>0 mins ago</td>
</tr>
<tr>
<td>Android System</td>
<td>fine location, coarse location</td>
<td>1 min ago</td>
</tr>
<tr>
<td>The Weather Channel</td>
<td>fine location, coarse location</td>
<td>2 mins ago</td>
</tr>
<tr>
<td>Facebook</td>
<td>cell scan, fine location, GPS, coarse location, wi-fi scan</td>
<td>17 mins ago</td>
</tr>
<tr>
<td>GO SMS Pro Theme Butterfly</td>
<td>fine location, coarse location</td>
<td>August 28</td>
</tr>
<tr>
<td>Settings</td>
<td>wi-fi scan, coarse location, fine location</td>
<td>June 16</td>
</tr>
<tr>
<td>Piano Tiles</td>
<td>wi-fi scan, coarse location</td>
<td>May 5</td>
</tr>
</tbody>
</table>
Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging

H Almuhimedi, F Schaub, N Sadeh, I Adjerid, A Acquisti, J Gluck, ...

CHI '15: ACM CHI Conference on Human Factors in Computing Systems
2014: Android layered the permissions

- Location now represents all types of location
- “Network” permissions no longer on top layer

Googe Play Store, Oct 19, 2014
https://support.google.com/googleplay/answer/6014972?p=app_permissions&rd=1
iOS8 privacy settings

- Limit Ad tracking
- Developers required to include a purpose string
- More “data classes”:
  - Location
  - Contacts
  - Calendar
  - Reminders
  - Photos
  - Camera
  - Microphone
  - Health Kit
  - Motion Activity
  - Social
A large chunk of the data-sharing ecosystem is invisible

<table>
<thead>
<tr>
<th>Destination</th>
<th>Location</th>
<th>Phone ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>jumptap.com</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>flurry.com</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>appads.com</td>
<td></td>
<td>11</td>
</tr>
</tbody>
</table>
Recent Policy: FTC Staff Report

Mobile Privacy Disclosures
Building Trust Through Transparency

FTC Staff Report | February 2013
California Attorney General

PRIVACY ON THE GO
RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM

January 2013

Kamala D. Harris, Attorney General
California Department of Justice
App Developers Should…

• Data checklist for PII
• Avoid or limit PII
• Develop a privacy policy
• Limit data collection
• Limit data retention
• Special notices for unexpected data practices “to enable meaningful practices”
• Give users access
CONSUMER DATA PRIVACY IN A NETWORKED WORLD:
A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY

FEBRUARY 2012
Privacy Multistakeholder Process: Mobile Application Transparency

Topics/Subtopics:
- Internet Policy Task Force
- Privacy
- Internet Policy

Date:
February 21, 2013

This web page provides details on the NTIA-convened privacy multistakeholder process regarding mobile application transparency. On June 15, 2012, NTIA announced that the goal of the first multistakeholder process is to develop a code of conduct to provide transparency in how companies providing applications and interactive services for mobile devices handle personal data.
Multi-stakeholder process (MSHP)

- Open meetings
- MSHP vs. self-regulation
NTIA MSHP vs W3C

- Communication (email, in-person, etc.)
- Goal (Code of Conduct vs. tech standard)
- Novelty of MSHP

Credits – Michael Heiss / FlickR
NTIA Code of Conduct: Data Types

- **Biometrics** (information about your body, including fingerprints, facial recognition, signatures and/or voice print.)

- **Browser History and Phone or Text Log** (A list of websites visited, or the calls or texts made or received.)

- **Contacts** (including list of contacts, social networking connections or their phone numbers, postal, email and text addresses.)

- **Financial Information** (Includes credit, bank and consumer-specific financial information such as transaction data.)

- **Health, Medical or Therapy Information** (including health claims and information used to measure health or wellness.)

- **Location** (precise past or current location and history of where a user has gone.)

- **User Files** (files stored on the device that contain your content, such as calendar, photos, text, or video.)
NTIA Code of Conduct: Third-Party Entities

- Ad Networks (Companies that display ads to you through apps.)
- Carriers (Companies that provide mobile connections.)
- Consumer Data Resellers (Companies that sell consumer information to other companies for multiple purposes including offering products and services that may interest you.)
- Data Analytics Providers (Companies that collect and analyze your data.)
- Government Entities (Any sharing with the government except where required or expressly permitted by law.)
- Operating Systems and Platforms (Software companies that power your device, app stores, and companies that provide common tools and information for apps about app consumers.)
- Other Apps (Other apps of companies that the consumer may not have a relationship with)
- Social Networks (Companies that connect individuals around common interests and facilitate sharing.)
What is the research question?

- Can users understand the terms used in the NTIA short form policy?

- How can we find the answer?
A Case Study on the Role of Usability Studies in Developing Public Policy: Web Survey

- 791 participants from Amazon mturk
  - 51% female
  - Age 18-73 years (mean 33, std 11)

- Asked to categorize realistic app-sharing scenarios

Balebako et al. 2014 USEC
Scenario example

The SuperTax app lets you fill out and submit your tax forms quickly and easily.

SuperTax will take a picture of your W-2. It will answer questions about your financial information, including salary and interest income.

It will then submit your return to state and federal agencies.

The scenarios describe the data collection and sharing completely, so you do not need to guess anything outside of what is described.

16. For each data collected by the app, what type of data is it?

<table>
<thead>
<tr>
<th></th>
<th>Biometrics</th>
<th>Browser History or Text Log</th>
<th>Contacts</th>
<th>Financial Information</th>
<th>Health, Medical or Therapy Information</th>
<th>Location</th>
<th>User Files</th>
<th>None of the Above</th>
<th>Not Sure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Photo of W-2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Salary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interest Income</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The different types of entities with which data can be shared are defined as follows:

- Ad Networks (Companies that display ads to you through apps.)
- Carriers (Companies that provide mobile connections.)
- Consumer Data Resellers (Companies that buy and/or sell consumer information to other companies for multiple purposes including offering products and services that may interest you.)
- Data Analytics Providers (Companies that collect and analyze your data.)
- Government Entities (Any sharing with the government except where required or expressly permitted by law.)
- Operating Systems and Platforms (Software companies that power your device, app stores, and companies that provide common tools and information for apps about app consumers.)
- Other Apps (Other apps of companies that the consumer may not have a relationship with)
- Social Networks (Companies that connect individuals around common interests and facilitate sharing.)
Users struggled to understand the terms

- Participants had high common understanding of:
  - Facebook = Social Network
  - Government Entities
  - Carriers

- Participants had low common understanding of:
  - Consumer Data Reseller
  - Data Analytics Providers
  - Ad Networks
Why was the result of the NTIA MSHP so bad?

- Process Fatigue
- What is usability?
- Cost of usability tests
- Process issues
Different Study
Current permissions requests are not sufficient for informed choice
What is the research question?

• Does timing impact whether privacy notices are effective?
• What do we mean by effective?
• What do we mean by timing?
What makes a privacy notice effective?

• The notice should have information people care about.

• A privacy notice should be salient; people should notice it.
  – Recall is a measure of salience
Contributions from this paper

• Salience of smartphone privacy notices can be improved through timing

• We provide recommendations on how to integrate privacy notices into apps for improved recall

• We provide design guidelines for improving privacy notices in the app store
Does timing matter? Which option is best?

- Smartphone apps can display privacy notices at many points
  - In the app store
  - During install
  - Before use
  - During use
  - After use

  Before app is on the phone
  App is on the phone and in use
Method to measure impact of timing on recall

1. Participants completed consent form and demographic questions
2. Installed and played the app
3. Experienced a distractor or delay
4. Answered recall questions
5. Evaluated the notice
Simple app quiz on American inventors

**Question 10 of 11**

Madame C. J. Walker (1867-1919) was the first African-American female millionaire. Her business included products she invented such as:

- bifocals
- the parachute
- **the lightening rod**
- hair-growing lotion

Oops!! The correct answer is "hair-growing lotion"

NEXT
The privacy notice

**What do we collect?**

- **Browser History**: A list of websites visited, or the calls or texts made or received.

**Who do we share with?**

- **Ad Networks**: Companies that display ads to you through apps.
Web survey used iFrame to mimic smartphone
Participants were assigned to a timing condition

- Not Shown
- App Store
- Before use
- During use
- After use
We approached this problem using both web surveys and a field experiment

- Web Survey (277 Mturk participants)
  - Participants played a virtual app online
- Field Experiment (126 participants)
  - Participants downloaded and played an app quiz

Same timing conditions
A Follow-up web survey used new conditions

• Web Survey (277 Mturk participants)
  – Participants played a virtual app online

• Field Experiment (126 participants)
  – Participants downloaded and played an app quiz

• Follow-up Web Survey (326 participants)
  – Participants played a virtual app online
All participants completed following steps

1. Completed consent form and demographic questions
2. Installed and played the app
3. Experienced a distractor or delay
   - Web survey: questions about privacy preferences
   - Field experiment: 24 hours
4. Answered recall questions
5. Evaluated the notice
Rate of Recall for Notice – Web Survey

Rate of correct recalls

- Not shown
- App store
- Before use
- During use
- After use
Rate of Recall for Notice – Field Study

- Not shown
- App store
- Before use
- During use
- After use

Rate of correct recall:
- 0%
- 5%
- 10%
- 15%
- 20%
- 25%
- 30%
- 35%
- 40%
Participants wanted to remember what was in notice

I would want notifications like this when I download or use an app
The privacy notice gave me information I care about
It is important for me to remember what the notification says over time
I was surprised by what I learned from the privacy notification
This notification could be improved so I understand it better
I expected the app to collect my browser history and share it with ad networks.
Why did app store perform so poorly?
New notices better, but not as good as during use

![Bar chart showing rates of correct recall for different display types]

- Not shown
- App store
- App store big
- App store popup
- During use
Design recommendations

• Participants remembered notices shown during app use
• Participants did not like the notices shown after app use
• Making the notice more prominent in the app store can improve recall
• Show privacy notices during app use, in context.
Different Study
App Developer decisions

- Privacy and Security features compete with
  - Features requested by customers
  - Data requested by financers
  - Revenue model
What is the research question?

• What are app developers doing to protect user privacy and security?

• What influences privacy and security decisions?
Research Project

• Exploratory Interviews

• Quantitative on-line study
Participant Recruitment

• 13 developers interviewed
• Recruited through craigslist and Meetups
• $20 for one-hour interview
Participant Demographics

- Variety of revenue models
  - Advertising
  - Subscription
  - Pay-per-use
  - Non-Profit
- Seven different states
- Small company size well-represented
Tools impact privacy and security

• Interviewees do:
  • Use cloud computing
  • Use authentication tools such as Facebook
  • Use analytics such as Google and Flurry
  • Use open source tools such as mysql
Tools not used

• Interviewees don’t use or are unaware of:
  • Use privacy policy generators
  • Use security audits
  • Read third-party privacy policies
  • Delete data
On-line surveys of app developers

• 228 app developers

• Paid $5 (avg: 15 minutes)

• Recruited through craigslist, reddit, Facebook, backpage.com

• Developer demographics
  – Majority were ‘Programmer or Software Engineer’ or ‘Product or Project Manager’
  – Avg age: 30 (18-50 years)
They collect a lot of data

<table>
<thead>
<tr>
<th>Behavior</th>
<th>Collect or Store</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters specific to my app</td>
<td>84%</td>
</tr>
<tr>
<td>Which apps are installed</td>
<td>74%</td>
</tr>
<tr>
<td>Location</td>
<td>72%</td>
</tr>
<tr>
<td>Sensor information (not location-related)</td>
<td>63%</td>
</tr>
<tr>
<td>Contacts</td>
<td>54%</td>
</tr>
<tr>
<td>Password</td>
<td>36%</td>
</tr>
</tbody>
</table>
Small companies less likely to show privacy and security behaviors
Small companies more likely to turn to social network or no one for advice
Findings

• Small companies lack privacy and security behaviors
  • Free or quick tools needed
  • Usable tools needed
• Small company developers rely on social ties for advice
  • Opportunities for intervention in social networks
• Legalese hinders reading and writing of privacy policies
• Third-Party tools heavily used
  • Third-party tools should be explicit about data handling