Privacy, Law, and Smartphones

Rebecca Balebako

Advisor: Dr. Lorrie Cranor
Agenda

• Quiz
• Reading discussion
• Permission notices on major platforms
• Policy on smartphone privacy
• (Recent research) Impact of timing on privacy notices
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
Discussion: Do apps on your phone

• Have privacy policy?
• Give you control/access over data collected?
• Have ‘Special Notices’?
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.
<table>
<thead>
<tr>
<th>App ops</th>
<th>LOCATION</th>
<th>PERSONAL</th>
<th>MESSAGING</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>
<td></td>
</tr>
<tr>
<td>Android System</td>
<td>fine location, coarse location</td>
<td>1 min ago</td>
<td></td>
</tr>
<tr>
<td>The Weather Channel</td>
<td>fine location, coarse location</td>
<td>2 mins ago</td>
<td></td>
</tr>
<tr>
<td>Facebook</td>
<td>cell scan, fine location, GPS, coarse location, wi-fi scan</td>
<td>17 mins ago</td>
<td></td>
</tr>
<tr>
<td>GO SMS Pro Theme Butterfly</td>
<td>fine location, coarse location</td>
<td>August 28</td>
<td></td>
</tr>
<tr>
<td>Settings</td>
<td>wi-fi scan, coarse location, fine location</td>
<td>June 16</td>
<td></td>
</tr>
<tr>
<td>Piano Tiles</td>
<td>wi-fi scan, coarse location</td>
<td>May 5</td>
<td></td>
</tr>
<tr>
<td>Messaging</td>
<td>read contacts</td>
<td>2 mins ago</td>
<td></td>
</tr>
<tr>
<td>Google Search</td>
<td>read contacts, read calendar</td>
<td>3 mins ago</td>
<td></td>
</tr>
<tr>
<td>Calendar Storage</td>
<td>read calendar, modify calendar</td>
<td>3 mins ago</td>
<td></td>
</tr>
<tr>
<td>Viber</td>
<td>read contacts, modify contacts, read call log</td>
<td>6 mins ago</td>
<td></td>
</tr>
<tr>
<td>Google Keyboard</td>
<td>read contacts</td>
<td>6 mins ago</td>
<td></td>
</tr>
<tr>
<td>GO SMS Pro</td>
<td>read contacts, read call log</td>
<td>6 mins ago</td>
<td></td>
</tr>
<tr>
<td>Facebook</td>
<td>read contacts</td>
<td>7 mins ago</td>
<td></td>
</tr>
</tbody>
</table>
Privacy Nudge

Did you know?
Your **location** has been shared 5398 times with Facebook, Groupon, GO Launcher EX, and 7 other apps for the past 14 days.

<table>
<thead>
<tr>
<th>App</th>
<th>Number of times</th>
<th>App</th>
<th>Number of times</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Play services</td>
<td>1603</td>
<td>Maps</td>
<td>18</td>
</tr>
<tr>
<td>Android System</td>
<td>1602</td>
<td>Viber</td>
<td>11</td>
</tr>
<tr>
<td>Groupon</td>
<td>1602</td>
<td>Facebook</td>
<td>5</td>
</tr>
<tr>
<td>Weather &amp; Clock Widget</td>
<td>296</td>
<td>Google Search</td>
<td>3</td>
</tr>
<tr>
<td>GO Launcher EX</td>
<td>255</td>
<td>MyFoodCoach Study</td>
<td>3</td>
</tr>
</tbody>
</table>

Let me change my settings
Keep sharing my location

Notification provided by AppOps.

Detailed Report

Hazim Almuhimedi, Florian Schaub, …
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

![Privacy Leaks]

How many times did Angry Birds leak information about you since 2012-07-26 5:20 PM?

<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
Developing Policy: NTIA MSHP

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
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.)
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
Impact of timing on recall of privacy notices

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

• Field Experiment (126 participants)
  – Participants downloaded and played an app quiz
Participants asked to recall the notice after a delay

1. Consent and demographic question

2. ‘Download’ and play app

3. Delay
   - Web survey: questions about privacy preferences
   - Field experiment: 24 hours

4. Answer recall questions about the app
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
Notice based on NTIA prototype

**US Inventors History Quiz**

**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.
Conditions varied only when notice was shown

- Not Shown
- App Store
- Before use
- During use
- After use
Participants remembered notices shown during app use

<table>
<thead>
<tr>
<th>Condition</th>
<th>Web Survey</th>
<th>Field Experiment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not shown</td>
<td>3%</td>
<td>9%</td>
</tr>
<tr>
<td>App store</td>
<td>17%</td>
<td>14%</td>
</tr>
<tr>
<td>Before use</td>
<td>37%*</td>
<td>33%*</td>
</tr>
<tr>
<td>During use</td>
<td>43%*</td>
<td>20%*</td>
</tr>
<tr>
<td>After use</td>
<td>28%*</td>
<td>37%*</td>
</tr>
</tbody>
</table>
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.
Participants remembered notices shown during app use

• Participants remember notices shown during app use

• Notice shown in app use had better recall than shown in app store

• Notice shown in app store was not significantly different than no notice
balebako@cmu.edu

Thanks!
Different Study
App Developer decisions

- Privacy and Security features compete with
  - Features requested by customers
  - Data requested by financers
  - Revenue model
Research Project

• Exploratory Interviews

• Quantitative on-line study
Findings

- Small companies lack privacy and security behaviors
- Small company developers rely on social ties for advice
- Legalese hinders reading and writing of privacy policies
- Third-Party tools heavily used
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