Privacy, Law, and Smartphones

Rebecca Balebako, PhD Candidate
Advisor: Dr. Lorrie Cranor
Privacy and Security Concerns

- Smartphone
- Privacy and Security
- Public Policy
Smartphones

• Increasingly popular

• Smartphones are different than personal computers:
  – Sensors
  – Always on
  – Immature
  – Smaller screens
Information on smartphones

Hidden Innovation in the GALAXY S4

GALAXY S4 gets you closer to what matters in life, bringing your world together.

- **RGB Light Sensor**
  - Measures the red, green, blue, and white intensity of the light source
  - *Samsung Adapt Display*

- **Rain Sensor**
  - Recognizes whether the cover is open or closed
  - *S View Cover*

- **Baryometer**
  - Identifies the atmospheric pressure at the user's current location
  - *S Health: Walking Mate*

- **Gesture Sensor**
  - Recognizes the user's hand movements using infrared rays
  - *Air Gesture*

- **Proximity Sensor**
  - Recognizes whether the mobile phone is located near the user by using infrared rays
  - *Direct Call*

- **Gyro Sensor**
  - Detects the mobile phone rotation state based on three axes
  - *Smart Rotation*

- **Accelerometer**
  - Detects the mobile phone movement state based on three axes
  - *S Health: Walking Mate*

- **Geomagnetic Sensor**
  - Detects magnetic field intensity based on three axes
  - *Digital Compass MAP*

- **Temperature Humidity Sensor**
  - Checks temperature and humidity levels
  - *S Health: Comfort Level*

SAMSUNG TOMORROW
Evaluating smartphone interfaces
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
Do apps on your phone:

• Have privacy policy
• Give you control/access over data collected
• Have ‘Special Notices’
Recent Policy: White House

CONSUMER DATA PRIVACY IN A NETWORKED WORLD:
A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY

FEBRUARY 2012
Recent Policy: FTC Staff Report
Developing Policy: NTIA MHP

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
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.)
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.)
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 and Phone 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>
Common understanding

<table>
<thead>
<tr>
<th>Fitness: Health Companies</th>
<th>Salsa: Ad Companies</th>
<th>Fitness: Sports Companies</th>
<th>Salsa: AdMeMetric</th>
</tr>
</thead>
<tbody>
<tr>
<td>HipClothes: Other Clothing Stores</td>
<td>GoodDriver: Car Rental</td>
<td>GoodDriver: Car Insurance</td>
<td>Bookstore: GreatReading</td>
</tr>
<tr>
<td>iTunes: Apple iCloud</td>
<td>FindMyKid: Parent’s Phone</td>
<td>CallCalendar: Google Calendar</td>
<td>GoodDriver: Traffic Data Company</td>
</tr>
<tr>
<td>FindMyKid: Local Police</td>
<td>Bookstore: Facebook</td>
<td>CallCalendar: Carrier</td>
<td>iTunes: Facebook</td>
</tr>
<tr>
<td>SuperTax: Federal Agency</td>
<td>EasyApply: State Agencies</td>
<td>SuperTax: State Agency</td>
<td></td>
</tr>
</tbody>
</table>

Legend:
- Ad Networks
- Carriers
- Government Entities
- Operating Systems and Platforms
- Consumer Data Resellers
- Data Analytics Providers
- Other Apps
- Social Networks
- None
- Not Sure
Why so bad?

• Process Fatigue
• What is usability?
• Cost of usability tests
• Process issues
Is Your Inseam a Biometric? Evaluating the Understandability of Mobile Privacy Notice

Technical reports: CMU-CyLab-13-011
Different Study
App Developers

- 200,000 iOS developers
- 800,000 iOS apps and 800,000 Android apps
- Low barrier to entry
Information on smartphones
App Developer study

- Exploratory Interviews (13)
- Quantitative on-line study (228)
Interview app developers

• How do they decide what privacy and security measures to take?
  – Search engines
  – Some training
  – Talk to friends
  – May have access to legal counsel
  – May need legal counsel
App developer tools

• Do
  – Cloud computing
  – Authentication (Facebook)
  – Analytics such as Google and Flurry
  – Open source tools such as mysql

• Don’t
  – Privacy Policy generators
  – Security audits
  – Read third-party privacy policies
  – Delete data
Quantitative Survey

• Behaviors:
  – Privacy Policy
  – CPO or equivalent
  – Encrypt stored data
  – Use SSL
  – Data minimization
Company size

Who do you turn to when you have questions about privacy and security:

- My social network (Friends, former colleagues)
- Developers from meetups or groups related to my work
- Lawyer outside my company
- Developers within my company
- Lawyer within my company
- Privacy/Security specialist within my company
- Other member of my company
- Trade association
- No one
<table>
<thead>
<tr>
<th>Data Type</th>
<th>Collect or Store</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters specific to my app</td>
<td>83.9%</td>
</tr>
<tr>
<td>Which apps are installed</td>
<td>73.9%</td>
</tr>
<tr>
<td>Location</td>
<td>71.6%</td>
</tr>
<tr>
<td>Advertising ID</td>
<td>70.6%</td>
</tr>
<tr>
<td>Sensor (not location)</td>
<td>63.0%</td>
</tr>
<tr>
<td>Phone Id</td>
<td>54.5%</td>
</tr>
<tr>
<td>Contacts</td>
<td>54.0%</td>
</tr>
<tr>
<td>Phone Number</td>
<td>44.1%</td>
</tr>
<tr>
<td>Password</td>
<td>35.5%</td>
</tr>
<tr>
<td>Credit Card Information</td>
<td>30.3%</td>
</tr>
</tbody>
</table>
Which category describes your app?
SECURITY SAYS YOUR EMPLOYEE LOCATOR DEVICE ISN’T TURNED ON.

MY WHAT?

I THINK YOU CALL IT A SMARTPHONE.

I MIGHT HAVE SOME QUESTIONS.

PUT THEM IN A TEXT TO YOURSELF. I’LL READ THEM LATER.
balebako@cmu.edu

Thanks!