21 - Privacy and security for mobile and ubicomp devices

Lorrie Cranor, Blase Ur, and Rich Shay

March 31, 2015

05-436 / 05-836 / 08-534 / 08-734
Usable Privacy and Security
Today!

- C-HIP/HITL
- Smartphone app notice and choice
- Privacy notice design space
- Activity: Notices for Google Glass
C-HIP Model

Communication-Human Information Processing Model

Human-in-the-loop framework
Apply HITL to Android Permissions

Communication Impediments
- Environmental Stimuli
- Interference

Communication

Personal Variables
- Demographics and Personal Characteristics
- Knowledge & Experience

Intentions
- Attitudes and Beliefs
- Motivation

Capabilities

Communication Delivery
- Attention Switch
- Attention Maintenance

Communication Processing
- Comprehension
- Knowledge Acquisition

Application
- Knowledge Retention
- Knowledge Transfer

Behavior
Current notices are not sufficient

- Users don’t understand what permissions mean
- Users don’t understand why permissions are being requested
- Users often click through without reading
Expert interviews

• We interviewed 20 experts from industry, academia, and government

• Asked them to describe smartphone security and privacy risks and mitigations

• Many harms could be addressed by better security practices

• Better privacy notices can address only a subset of these harms

App developers can protect users

• Best security practices
• Data minimization
• Understand privacy and security of third-party tools they use
• Transparency (privacy policies)
App developer study

• Interviewed 13 and surveyed 228 app developers

• Privacy and security not a high priority

• Small companies tend not to do much to protect security and privacy, rely on web searches and social networks for advice

• Developers use third-party tools without knowing privacy policies

• Many developers unfamiliar with privacy policy or don’t have privacy policy

App developer views on privacy policies

• “I haven’t even read [our privacy policy]. I mean, it’s just legal stuff that’s required, so I just put in there.”

• “I don’t see the time it would take to implement that over cutting and pasting someone else’s privacy policies.... I don’t see the value being such that that’s worth it.”
Multistakeholder Processes to Develop Enforceable Codes of Conduct
NTIA Code of conduct

• Developed through 1-year process
• Goal: Short-form privacy notice for apps
  – Inform app users about data collection
  – Improve transparency
  – Standardized notice
• Notice includes
  – 7 data types
  – 8 third-Party Entities
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.)
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.)
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.)
Usability test subgroup

• Never reached a consensus on what or how to test
• No usability testing ever occurred
Carnegie Mellon study

- Quick study to inform NTIA MSHP
- 791 participants recruited online (cost $913.35)
- 4 experts from NTIA MSHP
- 10 app scenarios
- Users read each scenario and tried to determine which data types and entities were described
- 2 conditions – with and without parentheticals

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 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>
Parenthetical condition

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.)

27. Apps can share data with different categories of entities. For each of the entities with which this app shares data, what category would best describe the entity?

<table>
<thead>
<tr>
<th></th>
<th>Ad Networks</th>
<th>Carriers</th>
<th>Consumer Data Resellers</th>
<th>Data Analytics Providers</th>
<th>Government Entities</th>
<th>Operating Systems and Platforms</th>
<th>Other Apps</th>
<th>Social Networks</th>
<th>None of the Above</th>
<th>Not Sure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State Agency</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Federal Agency</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Results

• All 4 experts agreed less than half the time
  – So unclear which answers are correct
• High agreement (>60% agreement) among online participants occurred less than half the time
• Parentheticals helped some, but some definitions were confusing
• Little evidence that these categories and definitions are well understood by users or experts
Impact of timing on recall of privacy notices

• Where can we put app privacy notices so they will be most effective?
  – In the app store?
  – After users download app?
  – After users start using app?
Conducted web survey and field experiment

- 277 survey participants played virtual app online and asked to recall privacy notice a minute later

- 126 field experiment participants downloaded and played app, and asked to recall privacy notice the next day
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

- 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

<table>
<thead>
<tr>
<th>Condition</th>
<th>Web Survey</th>
<th>Field</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>
Recommendations

• Better app privacy notices, informed by user studies
  – Meaningful terms and definitions
  – Placement where they will be noticed and read

• Security and privacy tools for app developers

• Better support for security and privacy from app platform providers
Privacy notice design space

- **Timing**
  - at setup
  - just in time
  - context-dependent
  - periodic
  - persistent
  - on demand

- **Channel**
  - primary
  - secondary
  - public

- **Modality**
  - visual
  - auditory
  - haptic
  - machine-readable

- **Control**
  - blocking
  - non-blocking
  - decoupled
Activity: Design a notice for people in the vicinity of Google Glass wearers