Android Permissions Remystified:  
A Field Study on Contextual Integrity

Primal Wijesekera (UBC)  
Arjun Baokar (UC Berkeley)  
Ashkan Hosseini (UC Berkeley)  
Serge Egelman (UC Berkeley)  
David Wagner (UC Berkeley)  
Konstantin Beznosov (UBC)
App permissions

**Storage**
Modify or delete the contents of your USB storage

**Phone calls**
Read phone status and identity

**Network communication**
Full network access

**Your location**
Approximate location (network-based)

ACCEPT
Why people make bad decisions

No comprehension
No contextual cues
User habituation

When to prompt

Action is **not reversible**.
Data is **sensitive**.
Incurs additional **cost**.

When to actually prompt

Privacy violations occur when *sensitive information* is used in ways *defying users’ expectations*.

### Android instrumentation

<table>
<thead>
<tr>
<th>Name</th>
<th>Log Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>API_FUNC</td>
</tr>
<tr>
<td>Permission</td>
<td>ACCESS_WIFI_STATE</td>
</tr>
<tr>
<td>Function</td>
<td>getScanResults()</td>
</tr>
<tr>
<td>App_Name</td>
<td>com.spotify.music</td>
</tr>
<tr>
<td>Timestamp</td>
<td>1412888326273</td>
</tr>
<tr>
<td>Visibility</td>
<td>FALSE</td>
</tr>
<tr>
<td>Screen</td>
<td>ON</td>
</tr>
<tr>
<td>Connectivity</td>
<td>NOT_CONNECTED</td>
</tr>
<tr>
<td>Location</td>
<td>Lat 37.xxxx&lt;br&gt;Long -122.xxxx&lt;br&gt;1412538686641</td>
</tr>
<tr>
<td>View</td>
<td>com.mobilityware.solitaire/.Solitaire</td>
</tr>
<tr>
<td>History</td>
<td>com.android.phone/.InCallScreen&lt;br&gt;com.android.launcher&lt;br&gt;com.android.mms/ConversationList</td>
</tr>
</tbody>
</table>
The experiment

36 Android smartphone users

6,048 hours of real-world use

27 million permission requests
Incorrect mental models

Invisible Permissions

- Background application (0.70%)
- Invisible service (14.40%)
- Screen off (60.00%)

Non-indicative Indicators

- Icon is visible for only 0.04% of accesses to location.
How often users should worry

8 requests per minute/user!
Location (10,960/day/user)
Reading SMS data (611/day/user)
Sending SMS (8/day/user)
Reading browser history (19/day/user)

4 exposes per minute/user!

Generally, every other permission request exposes data.

Does a user expect data exposure every 15 seconds?
Appropriateness of an information flow could be \textit{contextual}. 
<table>
<thead>
<tr>
<th>Name</th>
<th>Log Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>API_FUNC</td>
</tr>
<tr>
<td>Permission</td>
<td>ACCESS_WIFI_STATE</td>
</tr>
<tr>
<td>Function</td>
<td>getScanResults()</td>
</tr>
<tr>
<td>App_Name</td>
<td>com.spotify.music</td>
</tr>
<tr>
<td>Timestamp</td>
<td>1412888326273</td>
</tr>
<tr>
<td>Visibility</td>
<td>FALSE</td>
</tr>
<tr>
<td>Screen</td>
<td>ON</td>
</tr>
<tr>
<td>Connectivity</td>
<td>NOT_CONNECTED</td>
</tr>
<tr>
<td>Location</td>
<td>Lat 37.xxxx&lt;br&gt;Long -122.xxxx&lt;br&gt;1412538686641</td>
</tr>
<tr>
<td>View</td>
<td>com.mobilityware.solitaire./.Solitaire</td>
</tr>
<tr>
<td>History</td>
<td>com.android.phone./.InCallScreen&lt;br&gt;com.android.launcher&lt;br&gt;com.android.mms/ConversationList</td>
</tr>
</tbody>
</table>
1. Based on the screenshot, what were you doing on your phone?

2. Which of the following do you think the app was accessing?
   - [ ] Reading SMS stored in the phone
   - [ ] Reading the NFC Device
   - [ ] Sending a SMS
   - [ ] Scanning for WiFi
   - [ ] Reading browsing history
"When this photo was taken, the com.mobilityware.solitaire was Scanning for WiFi"

3. On a scale of 1–5 how much did you expect this app to be accessing this resource?
   - 1 (Least Expected)
   - 2
   - 3
   - 4
   - 5 (Most Expected)

4. If you were given the choice, would you have prevented the app from accessing this data?
   - Yes
   - No

5. Why?

   [Blank field]

6. Is it okay for the researchers to view this screenshot?
   - Yes
   - No
Users want a choice

80% of users would block at least one permission request.

35% of all requests were deemed inappropriate.
What matters

App visibility ( $r = 0.42$, $p < 0.001$ )

Users want to **vary decisions** based on the requesting app’s visibility.

Unexpected requests ( $r = -0.39$, $p < 0.018$)

**Defying expectations** violates the privacy.
Why users want to block permissions

“It wasn’t doing anything that needed my current location.”

53% of denied permissions were perceived as functionally irrelevant.

“I am not comfortable with you seeing my text messages”

32% of denied permissions were privacy sensitive.
We are not there yet

483 requests / hour
[Permission Requests]

213 requests / hour
[Actual Exposing Functions]

75 requests / hour
[Users wanted to block]
Ask-on-First-Use

User Agreement

\{\text{Application, Permission}\} : 51.3\% \\
\{\text{Application, Permission, Visibility}\} : 83.5\% \\

Number of prompts (during study period)

Pair : 16 / user \\
Triplet : 29 / user
Privacy is personal

Regression Model

Screen on: visibility, application, user (AUC=0.7)
Screen off: permission, application, user (AUC=0.8)

Different users have different preferences.
One size-fit-all policy will not be effective.
Lessons learned

**Visibility** of the application requesting permission is a strong contextual cue.

**Frequency** at which requests occur makes it impractical to prompt user on every case.

**Ask-on-first-use** can be extended to capture the context.