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

AndroidMPermTest

Click any button below to request the corresponding permission. A TextView will appear informing you about the request's result.

SMS

LOCATION

Allow **AndroidMPermTest** to access photos, media, and files on your device?

DENY ALLOW

Result:

Why people make bad decisions

No ***<u>comprehension</u>***

No ***<u>contextual cues</u>***

User ***<u>habituation</u>***

A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner. *Android Permissions: User Attention, Comprehension, and Behavior.* In Proceedings of the 2012 Symposium on Usable Privacy and Security.

A. P. Felt, E. Chin, S. Hanna, D. Song, & D. Wagner. Android permissions demystified. In Proceedings of the 18th ACM conference on Computer and communications security. ACM.

When to prompt

Action is ***not reversible***.

Data is ***sensitive***.

Incurs additional ***cost***.

A. P. Felt, S. Egelman, M. Finifter, D. Akhawe, and D. Wagner. *How to Ask for Permission.* Proceedings of the USENIX Workshop on Hot Topics in Computer Security (HotSec), 2012.

When to actually prompt

&

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

Helen Nissenbaum, *Privacy as Contextual Integrity*. Washington Law Review 79, 2004.

Android instrumentation

Name	Log Data
Type	API_FUNC
Permission	ACCESS_WIFI_STATE
Function	getScanResults()
App_Name	com.spotify.music
Timestamp	1412888326273
Visibility	FALSE
Screen	ON
Connectivity	NOT_CONNECTED
Location	Lat 37.xxxx Long -122.xxxx 1412538686641
View	com.mobilityware.solitaire/.Solitaire
History	com.android.phone/.InCallScreen com.android.launcher com.android.mms/ConversationList

The experiment

36 Android smartphone users

6,048 hours of real-world use

27 million permission requests

Incorrect mental models

Invisible Permissions

75.1%

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!

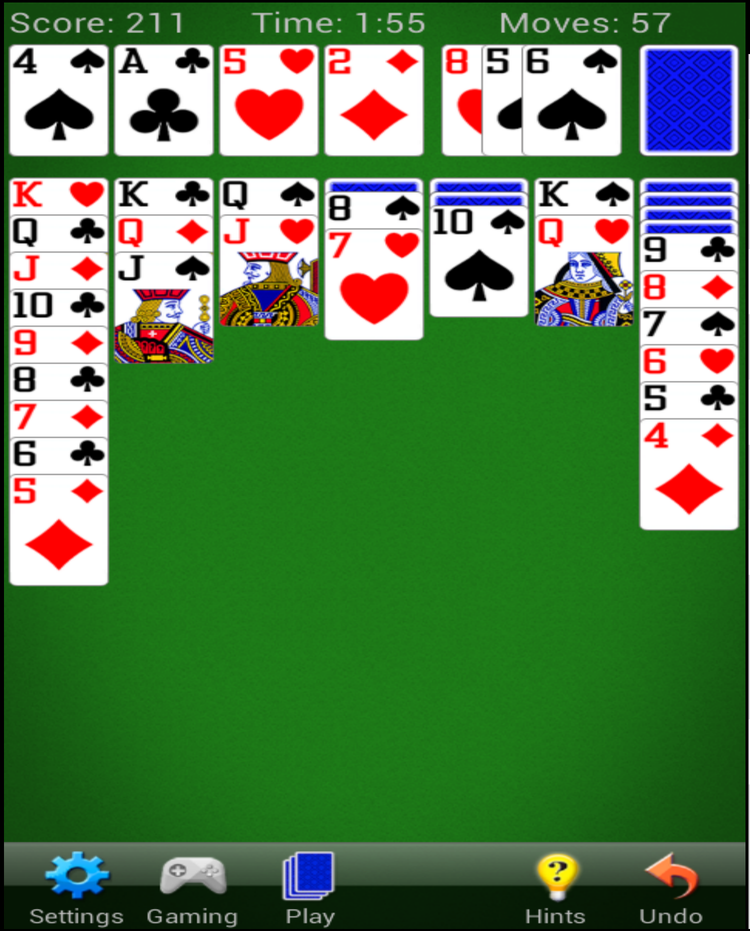
Location (10,960/day/user)
Reading SMS data (611/day/user)
Sending SMS (8/day/user)
Reading browser history (19/day/user)

4 exposes per minute/user!

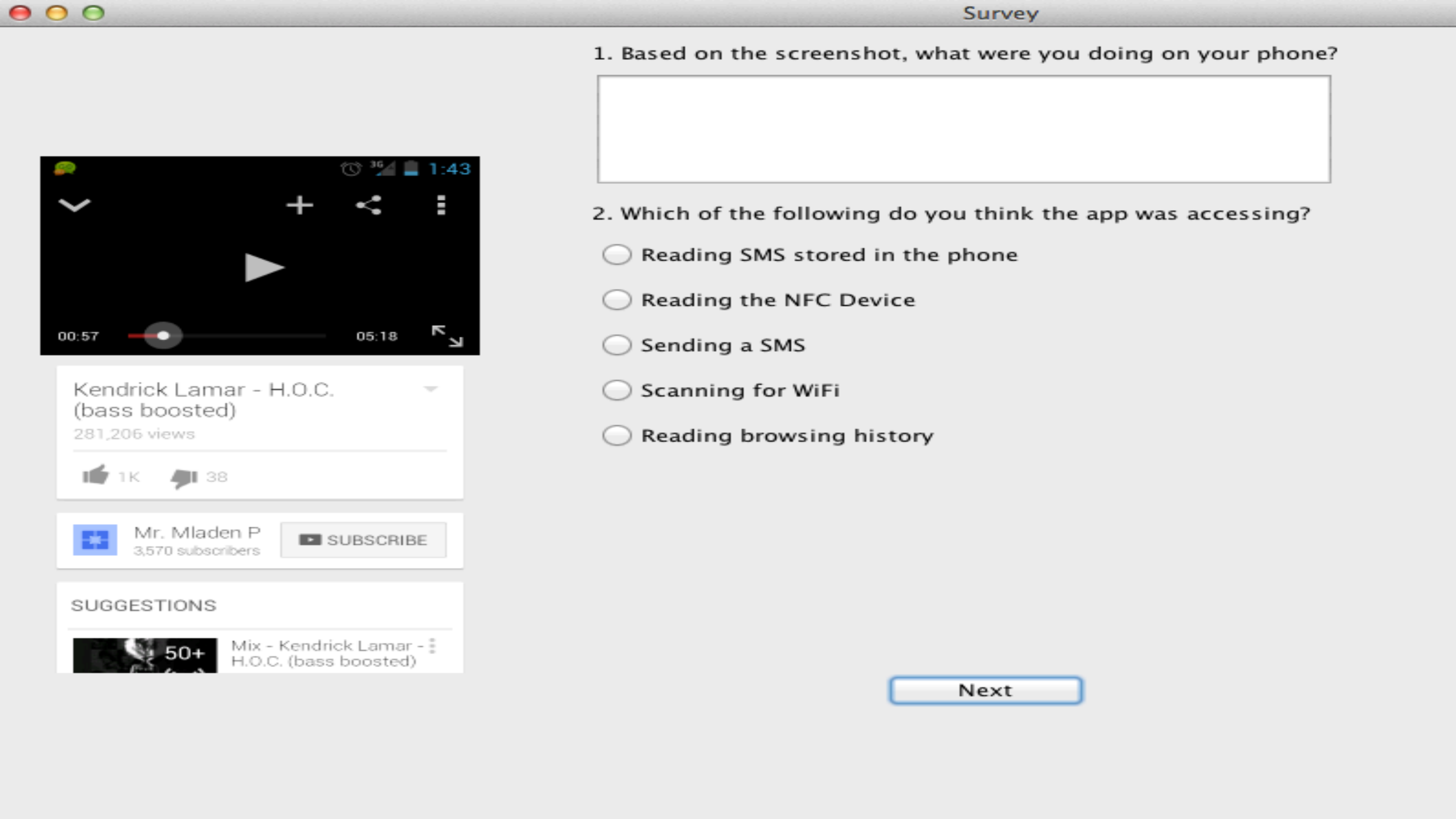
Generally, every other permission request exposes data.

Does a user expect data exposure every 15 seconds?

Appropriateness of an information flow could be ***contextual***.



Name	Log Data
Type	API_FUNC
Permission	ACCESS_WIFI_STATE
Function	getScanResults()
App_Name	com.spotify.music
Timestamp	1412888326273
Visibility	FALSE
Screen	ON
Connectivity	NOT_CONNECTED
Location	Lat 37.xxxx Long -122.xxxx 1412538686641
View	com.mobilityware.solitaire/.Solitaire
History	com.android.phone/.InCallScreen com.android.launcher com.android.mms/ConversationList



Survey

1. Based on the screenshot, what were you doing on your phone?

2. Which of the following do you think the app was accessing?

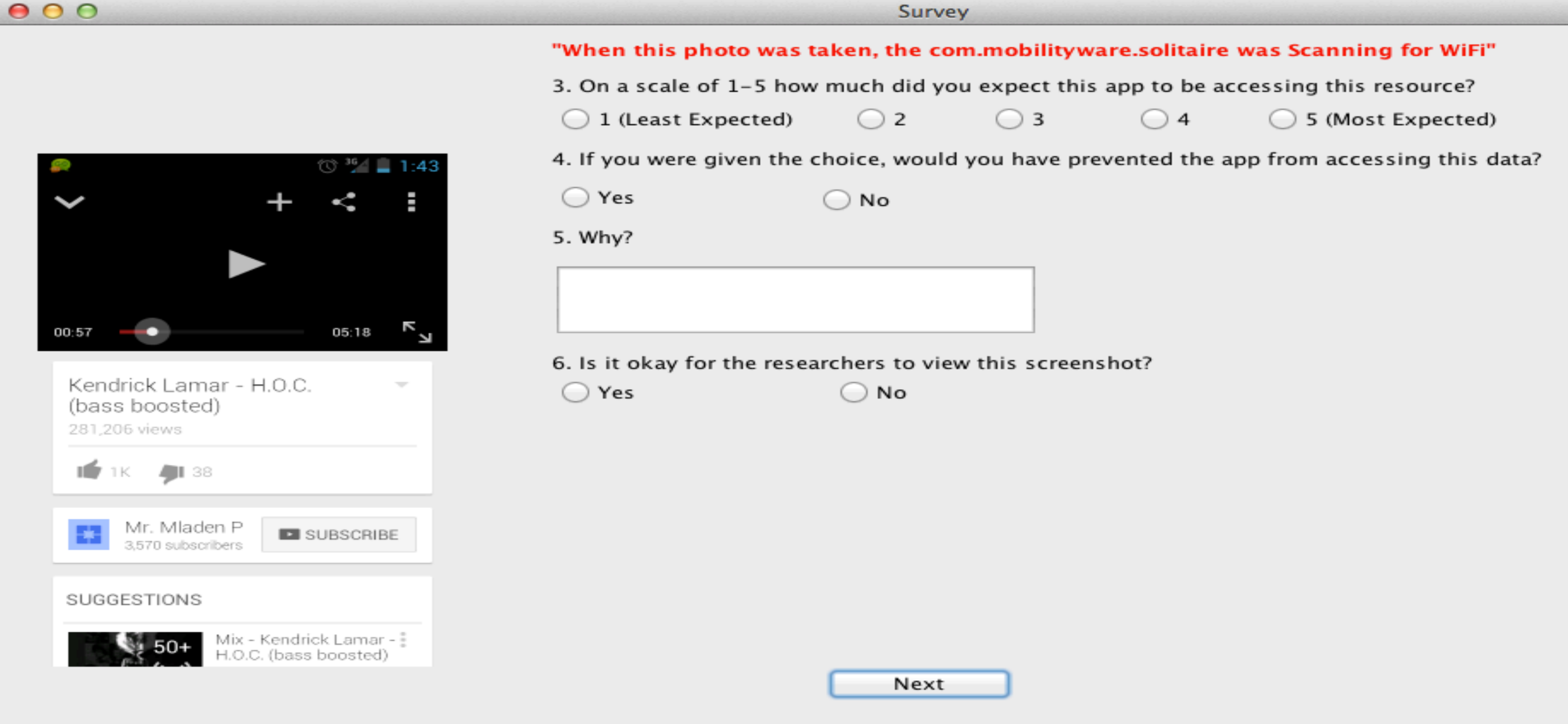
○ Reading SMS stored in the phone

○ 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?

6. Is it okay for the researchers to view this screenshot?

○ Yes ○ No

Next

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

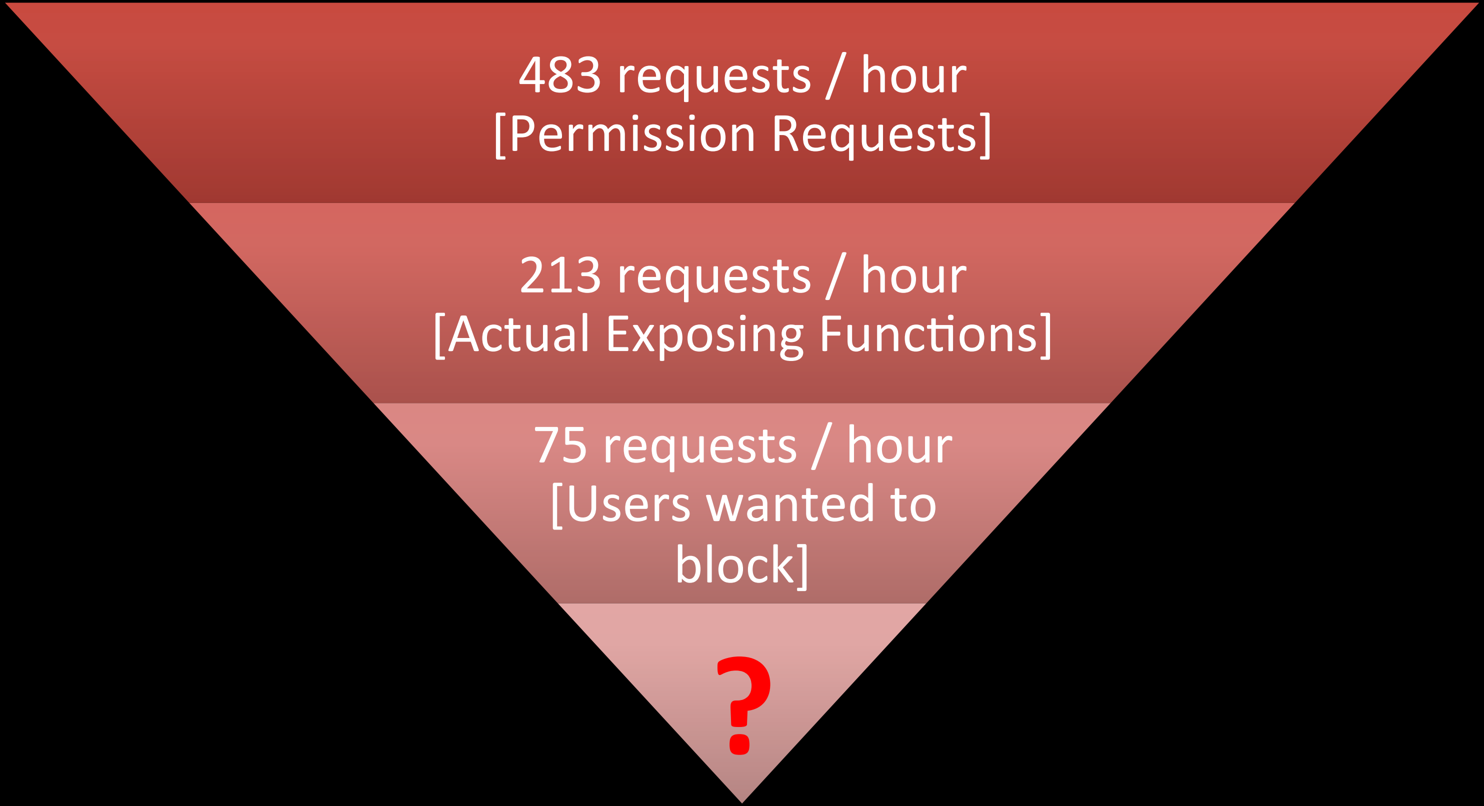
“It wasn’t doing anything that needed my current location.”

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

- {Application, Permission} : 51.3%
- {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.