

# A Large Scale Study of User Behavior, Expectations and Engagement with Android Permissions

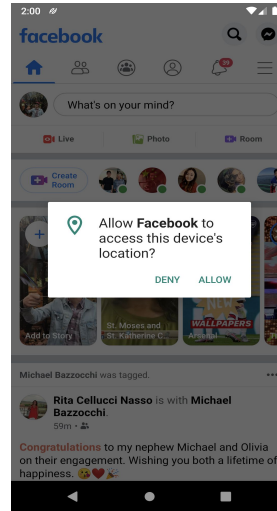
Weicheng Cao (U. Toronto) Chunqiu Xia (U. Toronto) Sai Teja Peddinti (Google)

David Lie (U. Toronto) Nina Taft (Google) Lisa M. Austin (U. Toronto)

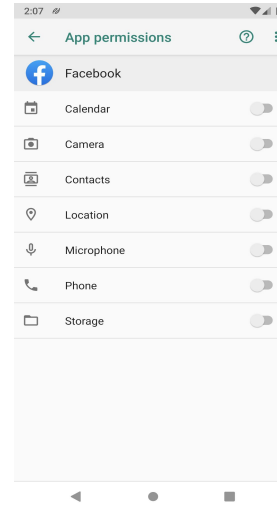
Published at USENIX Security '21

# Controlling private data sharing with Android Permissions

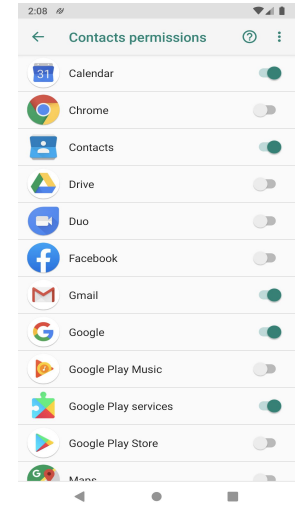
Users choose what **private data** to share with app via **Android permission system**



Runtime permission request

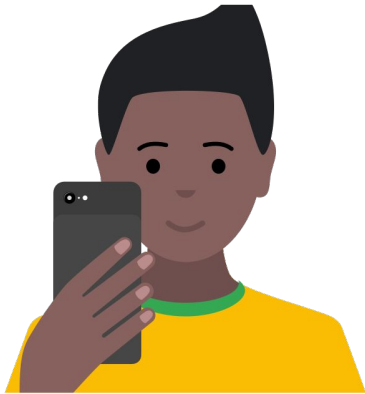


Android Settings menu



# Many factors affect user's decision to deny a permission

Demographic



Expectations

Attitudes

Explanations

GOAL:

Study the effect of one factor while controlling for others. Assess consistency of one factor's influence across all influencing factors.

CHALLENGES:

- collect these disparate types of data from the same individuals
- collect data from large, international set of participants

# Methodology

**Experience Sampling Method:** Survey participants right at the moment they made their choice.

## **Study Instrument:**

Created **PrivaDroid** app to obtain “in-the-wild” behavior data.

Participants install it on their personal phones and let it run in the background.

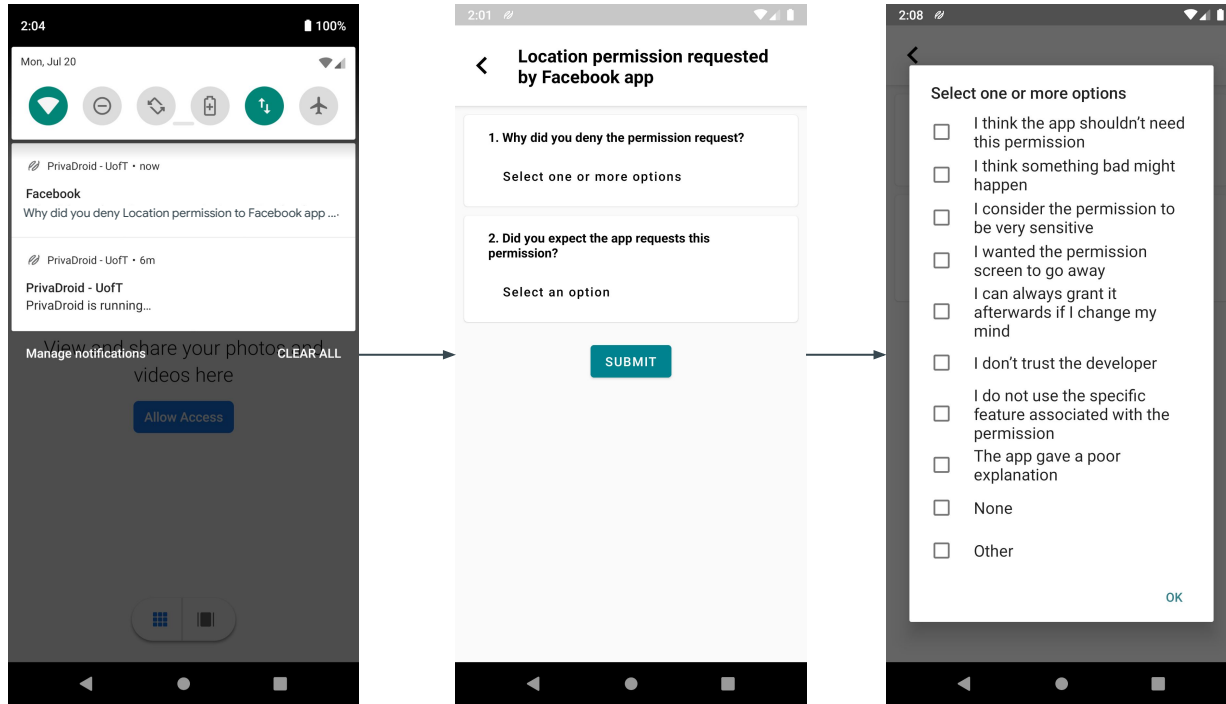
App observes specific **events**:

- App installation
- Granting / denying permission via dialog
- Granting / denying permission via settings

Launches **in-situ surveys** immediately.



# PrivaDroid as experiment tool



PrivaDroid was published on the Google Play Store until 2020 and supports all major **Android versions 6.0 to 10**, and is deployed in **4 popular languages**.

# Survey Design

- Demographic survey upon joining experiment
  - Asks about gender, age, education, and country.
- In-situ surveys right after app install and permission decision events
  - Captures participant's decision rationales, expectations and comfort level
  - 5 minutes cooldown between in-situ surveys
- Exit survey after 30 days
  - Adopted from IUIPC and updated to be more specific about “mobile privacy”
  - Control, Awareness, Collection and Secondary Use
  - Answered mapped to  $[-2, 2]$  and used to calculate privacy scores

# Participant Recruitment



**Become a participant by installing Android App**

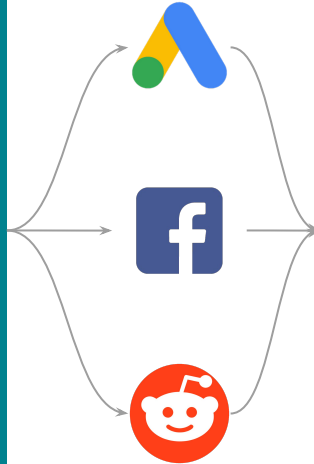
**Stay for 30 Days**

**\$10 Reward**

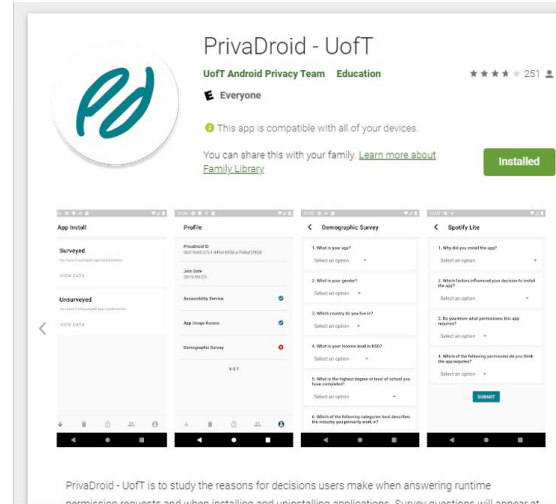
Experiment sponsored by the University of Toronto

The ad features icons for an Android phone, a calendar, and a money bag.

Online mobile Ad



Platforms

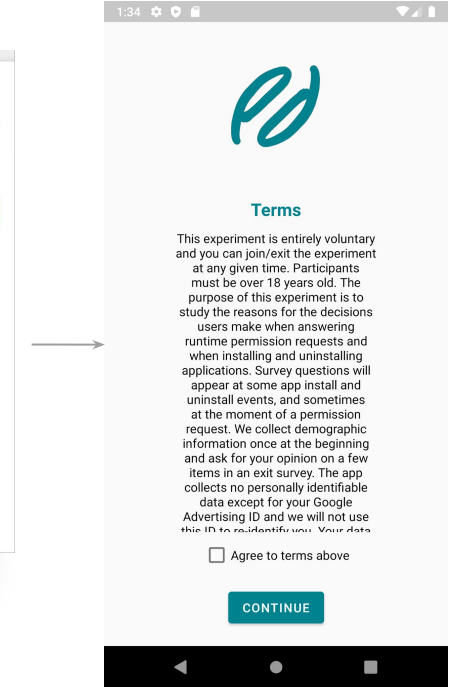


PrivaDroid - UoFT  
UoFT Android Privacy Team Education  
Everyone  
This app is compatible with all of your devices.  
You can share this with your family. [Learn more about Family Library](#) **Installed**

App Install, Profile, Demographic Survey, Specify Life

PrivaDroid - UoFT is to study the reasons for decisions users make when answering runtime permission requests and when installing and uninstalling applications. Survey questions will appear at

Google Play Store



1:34

**Terms**

This experiment is entirely voluntary and you can join/exit the experiment at any given time. Participants must be over 18 years old. The purpose of this experiment is to study the reasons for the decisions users make when answering runtime permission requests and when installing and uninstalling applications. Survey questions will appear at some app install and uninstall events, and sometimes at the moment of a permission request. We collect demographic information once at the beginning and ask for your opinion on a few items in an exit survey. The app collects no personally identifiable data except for your Google Advertising ID and we will not use this ID to re-identify you. Your data

Agree to terms above

**CONTINUE**

PrivaDroid App

# Study Summary

**Study Period:** Nov 2019 to May 2020

**Participant Study Duration:** 30 Days

**Participant compensation:** \$10 USD if they stayed for 30 days

**10 Countries & Regions:** Canada, United States, Argentina, United Kingdom, France, Spain, South Africa, India, Singapore, and Hong Kong.

**Money spent on advertising (for recruitment):** \$12,953.85 USD

5,377 installs of the PrivaDroid app, but only **1,719 participants** stayed for the required 30 day period and completed the study.

**72,214 app install events** of which 36% were surveyed, and **36,152 permission decision events** of which 30% were surveyed.



# What do we collect?

## **Demographics:**

Gender, age,  
education,  
country/region

## **Behavior:**

Grant/Deny decisions  
Apps installed

## **Expectations:**

Whether participants  
expected the permission  
request

## **Rationales:**

Why participants granted  
or denied a permission

## **Explanations:**

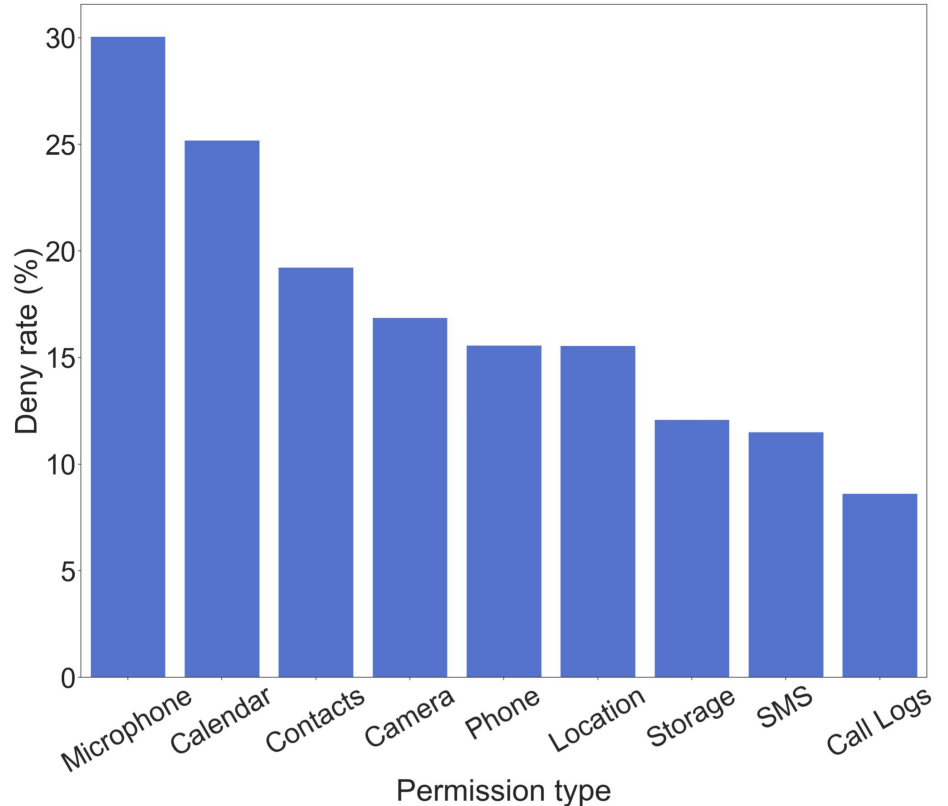
Apps' explanations in  
pre-prompts, for  
permissions

## **Attitudes:**

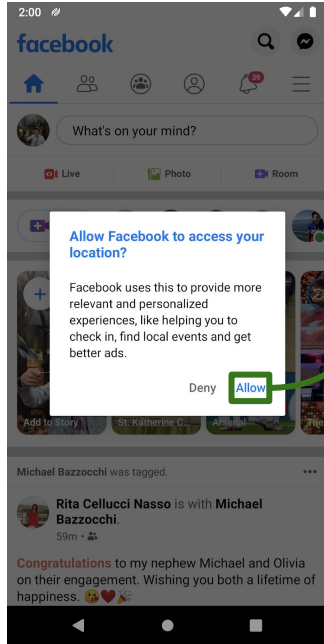
Privacy sensitivity scores

# Permission data summary

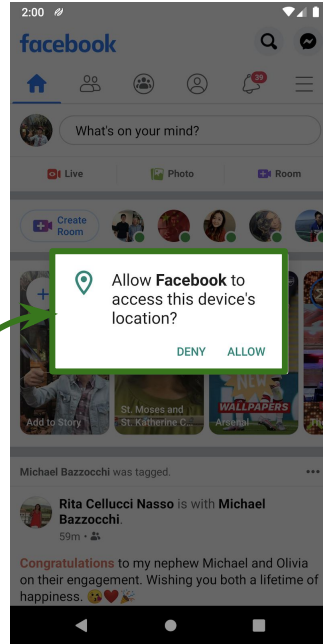
- ~36K permission decision events, 30% were surveyed
  - Overall 16.7% deny rate
  - 8% permission decisions from Settings menu
- Reasons for denying permissions
  - “I can always grant it afterwards if I change my mind” - 27%
  - “I do not use the specific feature associated with the permission” - 25%
  - “I think the app shouldn’t need this permission” - 23%



# Explanations



Explanation



Permission request

Explanation must have:

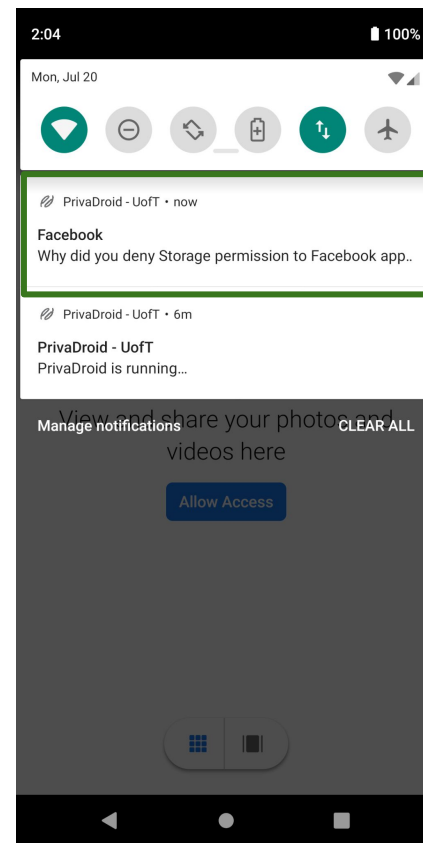
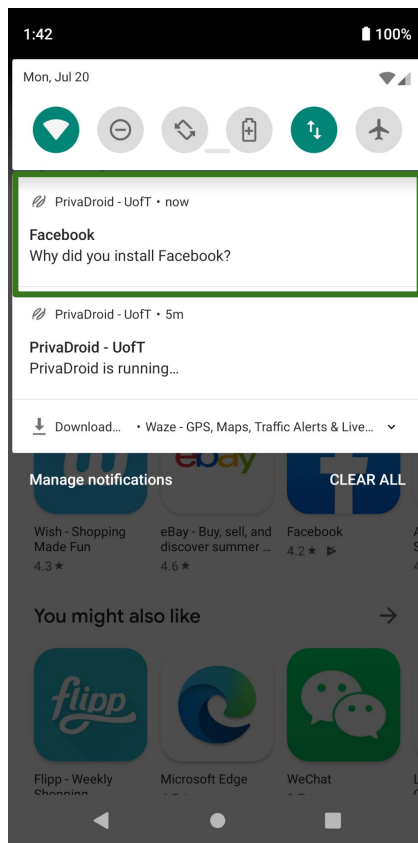
- A keyword about **data collection**, e.g. access, collect, etc.
- A keyword about a **permission/resource type**, e.g. camera, photos, etc.

Deny rate **15.4%** without explanation -> **7.1%** with explanation

Mixed effects logistic regression (MELR) shows presence of explanation reduces deny rate

# Expectations

We measure users' permission expectations at two points: install time and runtime.

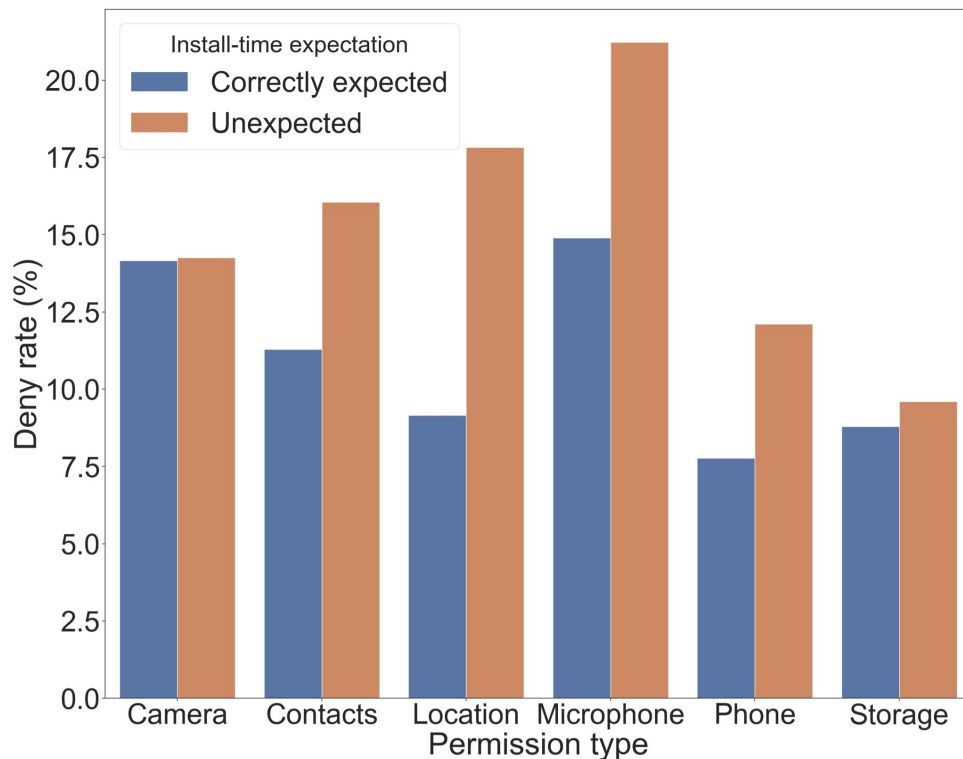


# (Install time) Expectations

Unexpected requests deny rate: 14.2%

Expected requests deny rate: 10.2%

MELR model shows unexpected install time requests significantly increase likelihood that a user denies a permission. Model shows this is true even when controlling for other factors.

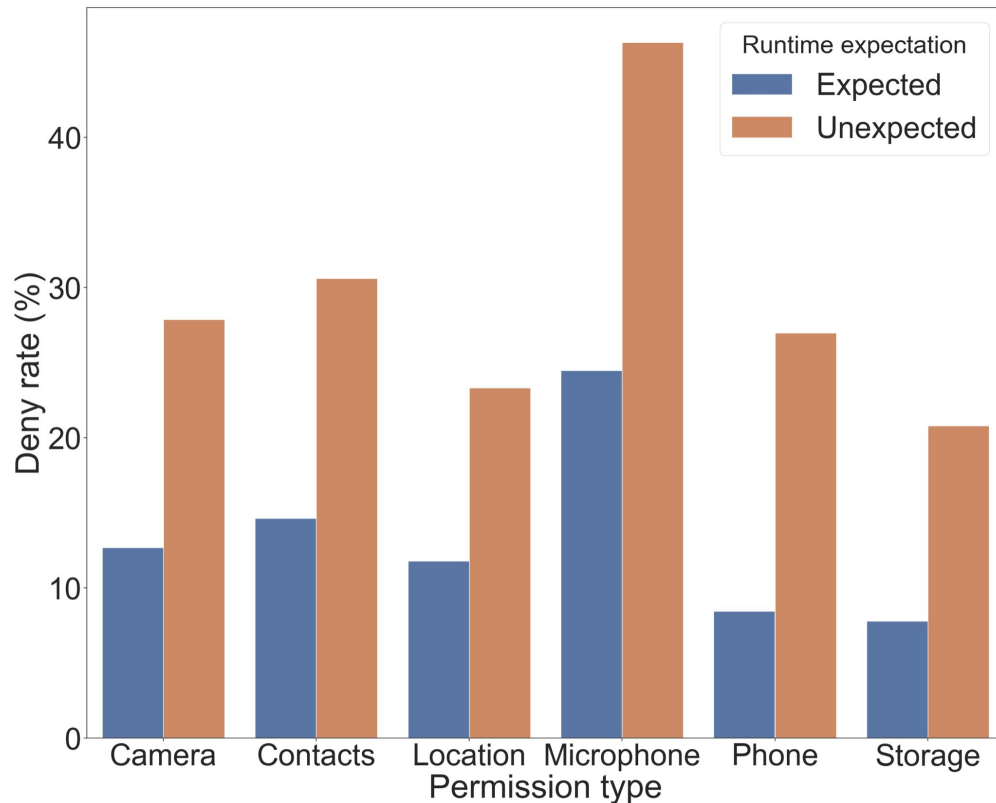


# (Runtime) Expectations

Unexpected requests deny rate: 26.9%

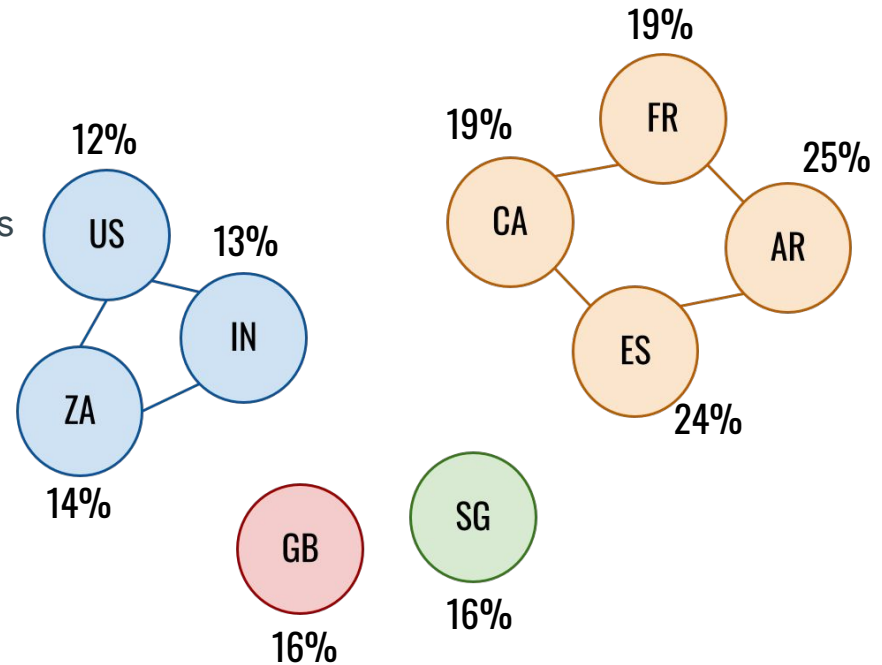
Expected requests deny rate: 12.2%

MELR model shows unexpected runtime requests significantly increase likelihood that a user denies a permission. Model shows this is true even when controlling for other factors.



# Cross country analysis

- Challenging to understand country to country comparison
  - Privacy attitudes, cultural values, regulatory frameworks, etc.
  - Only observations about the participants in our study
- Deny rates and distribution
  - **2 distinct cliques of countries** found via pairwise ANOVA tests on the deny rate distributions
  - Participants from countries in the same clique are drawn from populations with the **same mean deny rates**



HK is excluded because of not enough female participants

# Factors influencing deny rate

- Mixed effects logistic regression model with 12 features
  - Privacy sensitivity (4)
  - Explanation (1)
  - Runtime expectation (1)
  - Whether permission decision is in Settings menu or runtime (1)
  - Demographic variables (4)
  - Permission type (1)
- Participant and app are included as random effects
- Permission decision as the binary response variable ('1' represents a deny and '0' an accept)

Variance-Inflation Factors (VIF) analysis shows no coefficients are inflated due to multicollinearity. All VIFs values < 5.



Variable	Values	$\beta$ Coefficient (p-value)
control awareness	[-2, 2]	-0.044
<b>collection</b>	[-2, 2]	0.109
<b>secondary_use</b>	[-2, 2]	<b>0.404 (***)</b>
<b>has_explanation</b>	Binary	-0.725 (***)
<b>settings_menu</b>	Binary	2.04 (***)
country/region (reference: US)	<b>Canada</b>	0.870 (***)
	<b>Argentina</b>	0.555 (***)
	<b>UK</b>	0.567 (***)
	<b>France</b>	0.795 (***)
	<b>Spain</b>	0.883 (***)
	South Africa	0.068
	India	0.118
	Singapore	0.42 (.)
<b>gender</b> (reference: Male)	Female	0.299 (**)

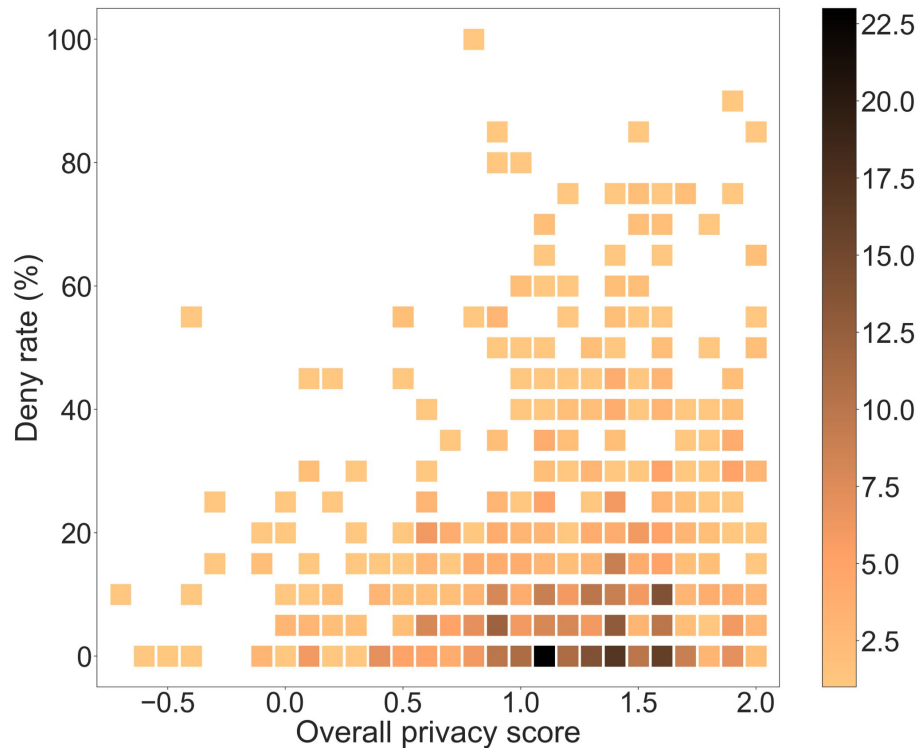
Variable	Values	$\beta$ Coefficient (p-value)
age (reference: Below 30 years)	Between 30 and 50	-0.104
	Above 50	-0.006
education (reference: Bachelor's degree)	<b>Less than high school</b>	-0.249 (*)
	High school or equivalent	-0.193
permission (reference: Location)	Calendar	0.259
	Camera	0.011
	<b>Contacts</b>	0.258 (**)
	<b>Microphone</b>	0.606 (***)
	Phone	-0.093
	SMS	-0.265
	<b>Storage</b>	-0.379 (***)
<b>runtime_expected</b> (reference: Yes)	No	1.216 (***)
	Not surveyed	0.306 (***)

Random Effect	Variance
App (intercept)	1.889
User (intercept)	1.785

Significance codes:  
 $p < 0.001$  (\*\*\*)  
 $p < 0.01$  (\*\*)  
 $p < 0.05$  (\*),  
 $p < 0.1$  (.)

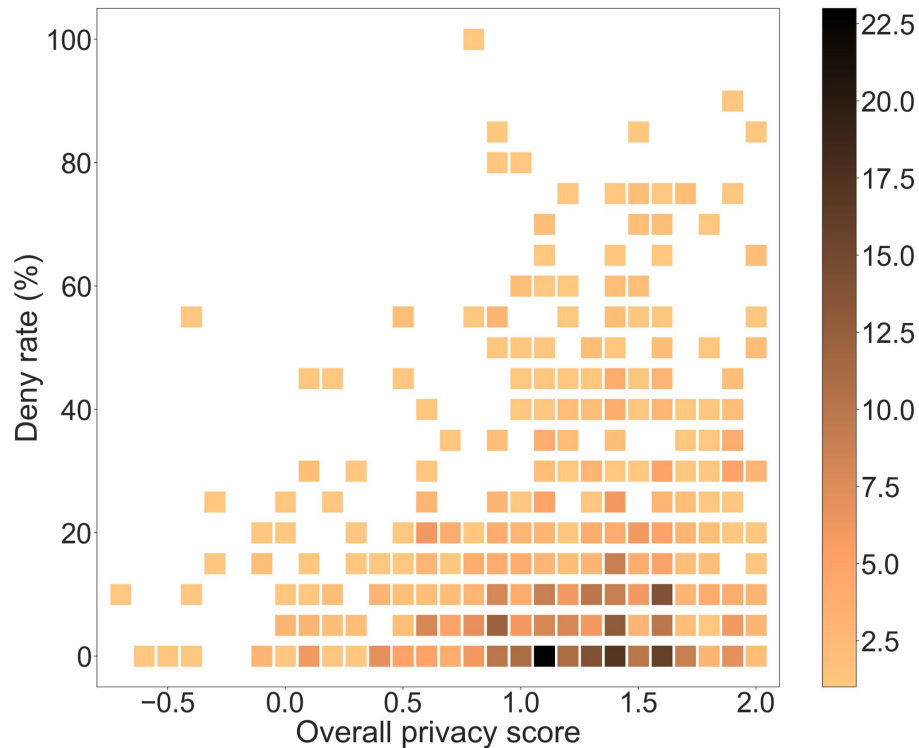
# Privacy Sensitivity and Deny Rate

- Overall privacy sensitivity = average(Control, Awareness, Collection, and Secondary Use)
- Each cell: # of participants for each (privacy sensitivity, deny rate) bucket



# Privacy Sensitivity and Deny Rate

- Three Observations:
  - Privacy score  $\uparrow$ , average deny rate  $\uparrow$
  - Privacy score  $\uparrow$ , variance  $\uparrow$  in permission denying behavior
  - For the high privacy score group (attitude), 29% participants have deny rate lower than mean of 16.7% (behavior) => Highly **engaged users** with better permission expectations.



# Limitations

- Selection Bias: Participants more likely to
  - Respond to mobile advertising
  - Be tolerant to data collection by a mobile app
  - Be incentivised by financial rewards
- Incomplete visibility:
  - Can't see events for apps before study period, such as pre-installed or popular apps
  - Not enough data to analyze behaviors of individual apps

# Conclusions

- Mobile advertising effective in recruiting participants
- Including rationales for permissions benefits the apps by reducing deny rate by more than half (7.1% vs 15.4%)
- Both install-time and runtime expectations affect users permission decisions
  - **this is true regardless of demographics and permission type**
- Participant demographics, their privacy attitudes, expectations, explanations and permission types all play a role in permission denial decision

Thank you!

Questions?