TurtleGuard: Helping Android Users Apply Contextual Privacy Preferences

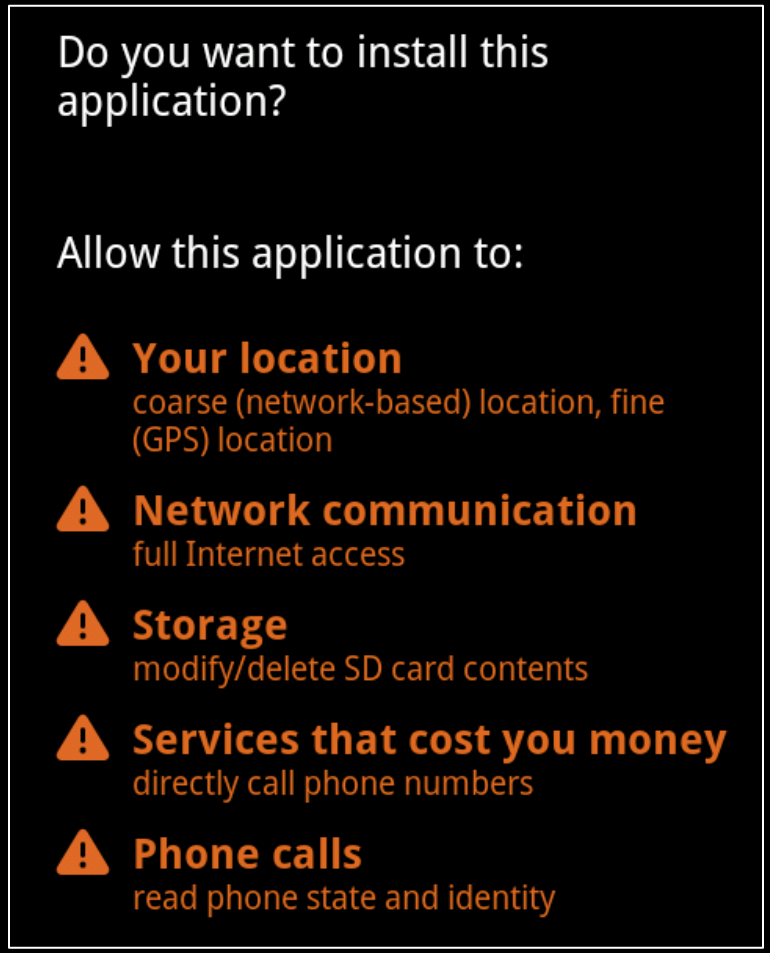
Lynn Tsai	UC Berkeley
Primal Wijesekera	University of British Columbia
Joel Reardon	UC Berkeley
Irwin Reyes	ICSI
Jung-Wei (Jennifer) Chen	Good Research
Nathan Good	Good Research
Serge Egelman	ICSI / UC Berkeley
David Wagner	UC Berkeley

HOW TO SHOW PRIVACY NOTICES ON MOBILE DEVICES?

comprehension study

online study of 308 Android users
- quantitative survey

laboratory study with 24 users
- think-aloud experiment
- semi-structured interviews



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 (SOUPS). **Best Paper Award!**

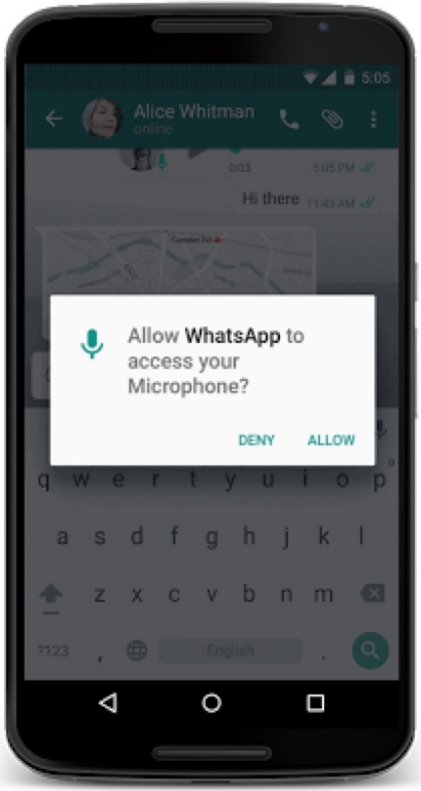
suggestions



– many were habituated—too many requests
– only show information when necessary



– many were unaware—too late in the process
– provide information prior to decision-making


5:05
Alice Whitman
online
Hi there
Allow WhatsApp to access your Microphone?
DENY
ALLOW


HOME
2:28 PM
100%
"Facebook" Would Like to Access Your Contacts
Don't Allow
OK

this ignores *context*

show privacy notices more than once, but

UNDER WHAT CIRCUMSTANCES?

how often are resources accessed *in practice*?

dynamic analysis

- modified Android OS and gave phones to 40 people
- hooked all API methods involving access to sensitive data

what are users doing when data is accessed (context)?

P. Wijesekera, A. Baokar, A. Hosseini, S. Egelman, D. Wagner, and K. Beznosov. Android Permissions Remystified: A Field Study on Contextual Integrity. Proceedings of the 24th USENIX Security Symposium, 2015.

the results

36 Android smartphone users

6,048 hours of real-world use

27 million permission requests

more runtime requests?

213 requests per hour!

- location (10,960/day)
- reading SMS data (611/day)
- sending SMS (8/day)
- reading browser history (19/day)

asking each time is infeasible

- …but 80% of participants wanted to block at least 1 request
- on average, they wanted to block 35% of all requests

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.

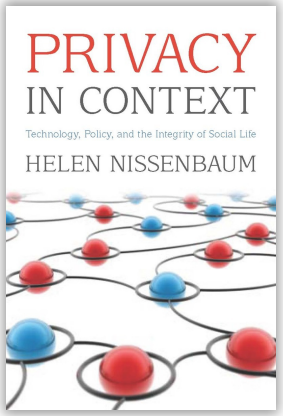
ask-on-first-use can be extended to capture the context.

privacy as contextual integrity

inappropriate data flows violate *contextual information norms*

contextual information norms are modeled using:

- data subject (i.e., the user)
- data sender
- data recipient
- information type
- transmission principle (constraints)



what does this mean for user-centered design?

notice should be shown in context

only provide notice when *reasonable* privacy expectations are likely to be violated

- don't bother the user about appropriate data flows
  …to prevent habituation
- do bother the user about unknown or inappropriate flows
  …to preserve contextual integrity

HOW CAN NOTICES BETTER ACCOUNT FOR CONTEXT?

notice in context

definitively determining context is impossible

…use proxies to approximate, and learn from mistakes

can we use machine learning to detect when context has changed from *expected* data use to *unexpected*?

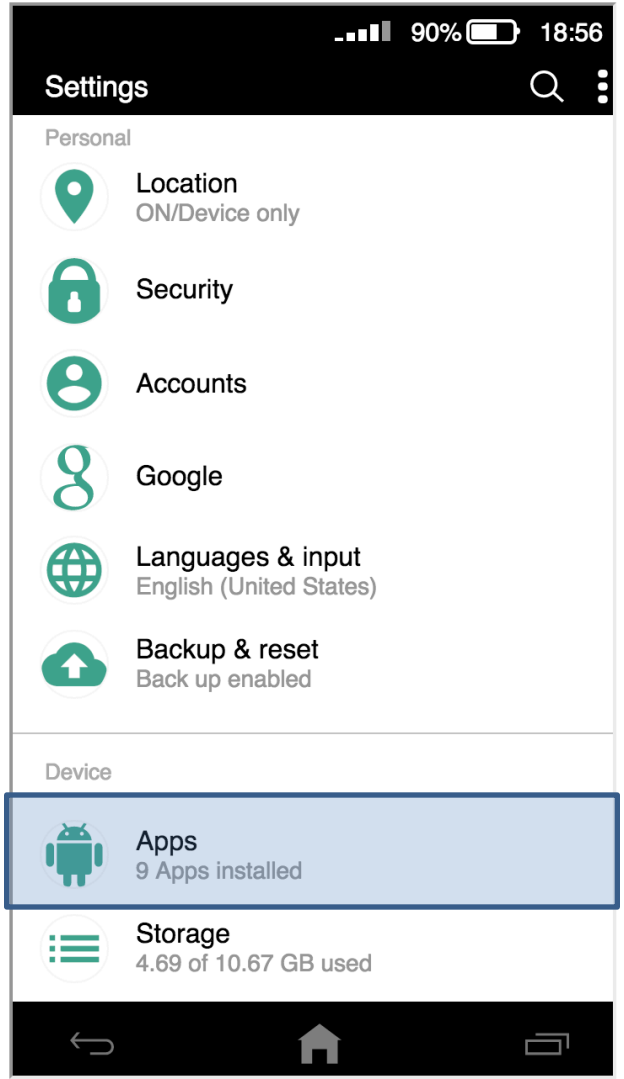
P. Wijesekera, A. Baokar, L. Tsai, J. Reardon, S. Egelman, D. Wagner, and K. Beznosov. *The Feasability of Dynamically Granted Permissions: Aligning Mobile Privacy with User Preferences*. In Proceedings of the 2017 IEEE Symposium on Security and Privacy (Oakland '17).

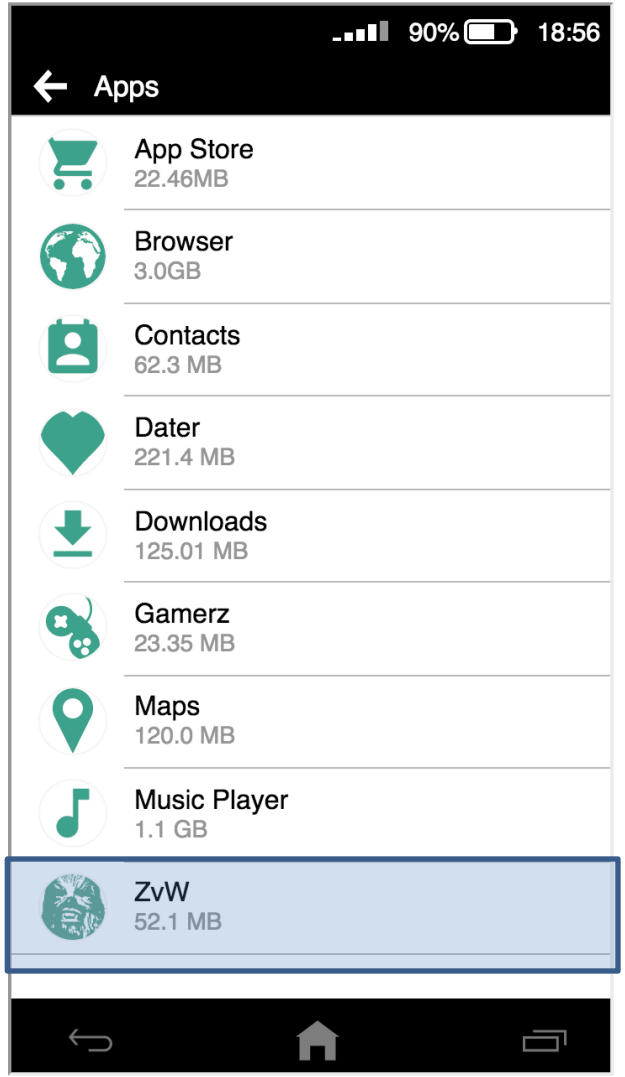
automatically regulating access

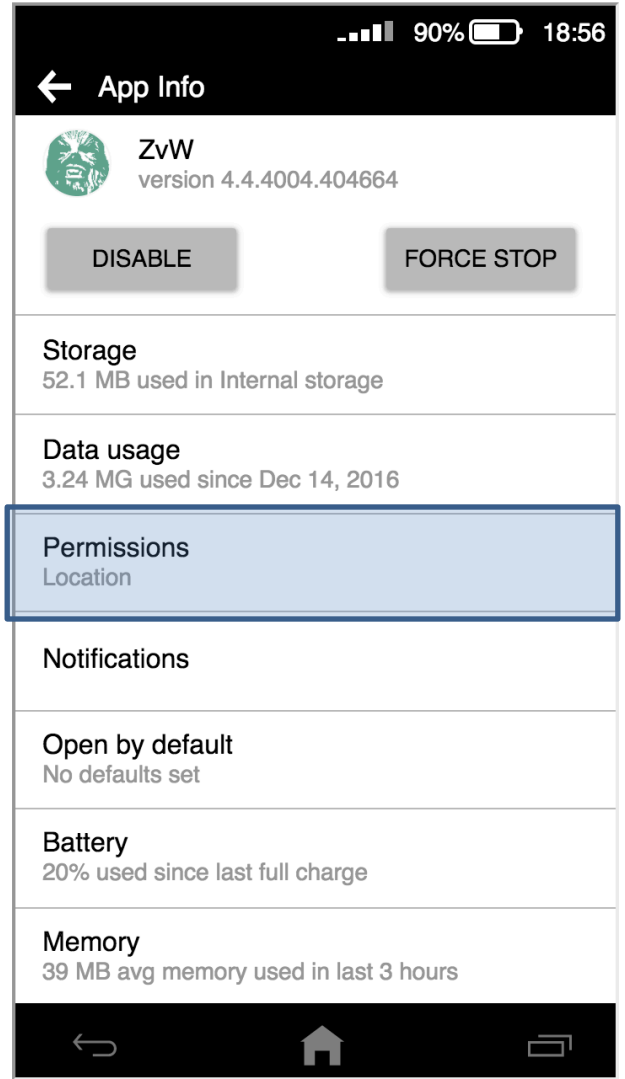
	Error Rate	Average Prompts/User
Ask-on-first-use (Android/iOS)	15.4%	12.34
ML Model	3.2%	12.00
ML Model (low-prompt)	7.4%	8.00

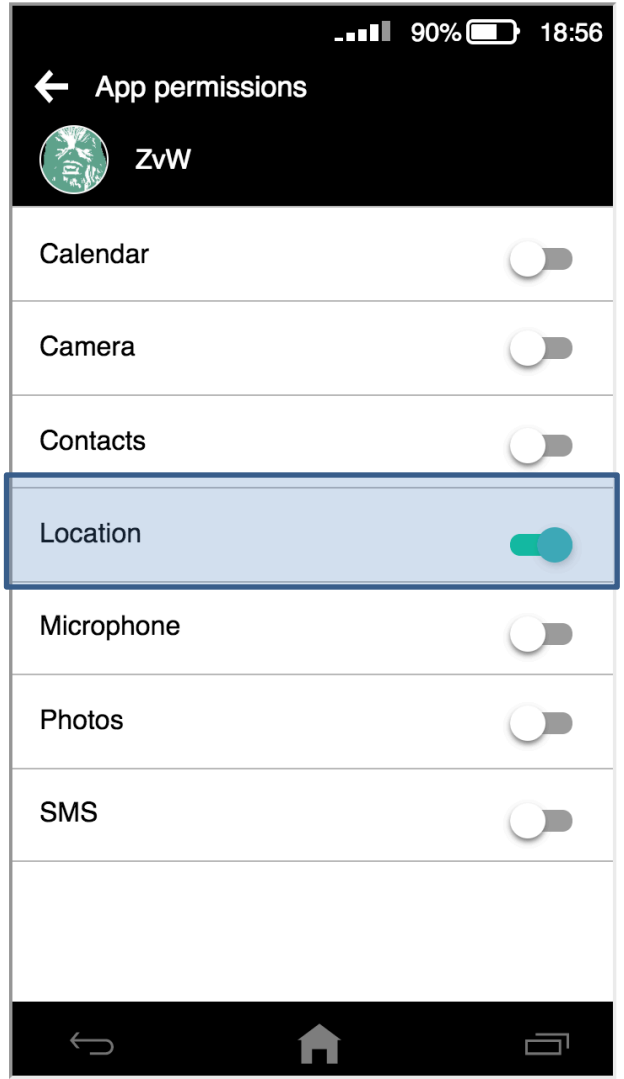
because the classifier isn’t perfect,

WHERE CAN USERS GO TO CORRECT ERRORS?


90%
18:56
Settings
Personal
Location
ON/Device only
Security
Accounts
Google
Languages & input
English (United States)
Backup & reset
Back up enabled
Device
Apps
9 Apps installed
Storage
4.69 of 10.67 GB used


90%
18:56
Apps
App Store
22.46MB
Browser
3.0GB
Contacts
62.3 MB
Dater
221.4 MB
Downloads
125.01 MB
Gamerz
23.35 MB
Maps
120.0 MB
Music Player
1.1 GB
ZvW
52.1 MB


90%
18:56
App Info
ZvW
version 4.4.4004.404664
DISABLE
FORCE STOP
Storage
52.1 MB used in Internal storage
Data usage
3.24 MG used since Dec 14, 2016
Permissions
Location
Notifications
Open by default
No defaults set
Battery
20% used since last full charge
Memory
39 MB avg memory used in last 3 hours


90%
18:56
App permissions
ZvW
Calendar
Camera
Contacts
Location
Microphone
Photos
SMS

status quo problems

1) no holistic view of what apps have accessed

2) per-app information is many layers down

3) permissions are not contextual

privacy dashboard

classifier reduces error rates five-fold

- *some* errors will always occur
- open question: acceptable error rate?

users need to be able to:

- understand automated decisions (auditing/error detection)
- change incorrect decisions (retraining)

dashboard user study

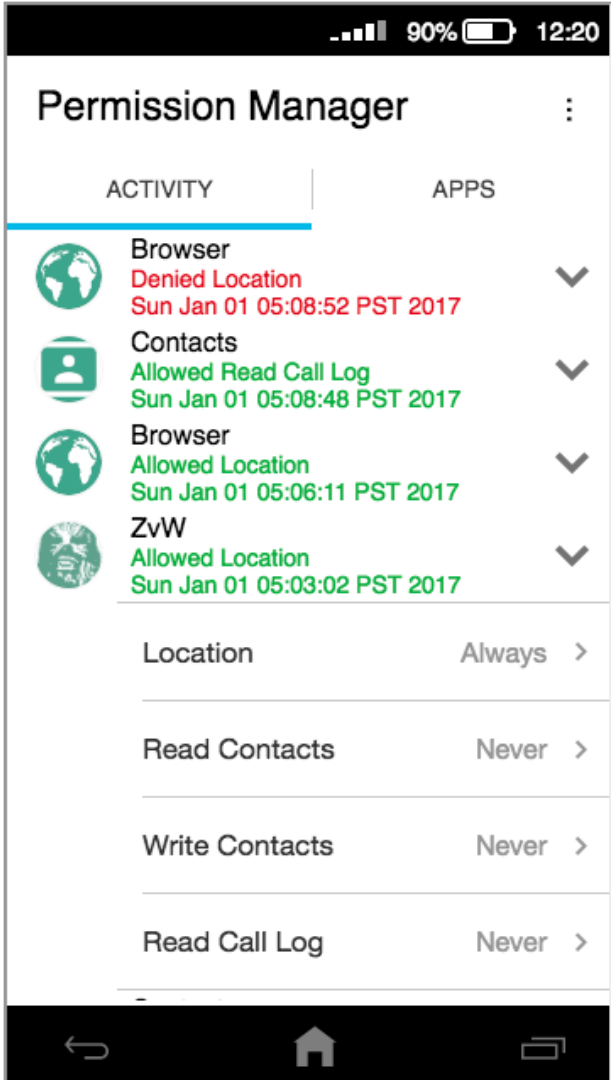
prior work showed <25% of users understand background applications have same abilities as foreground ones

does the dashboard correct this mental model?

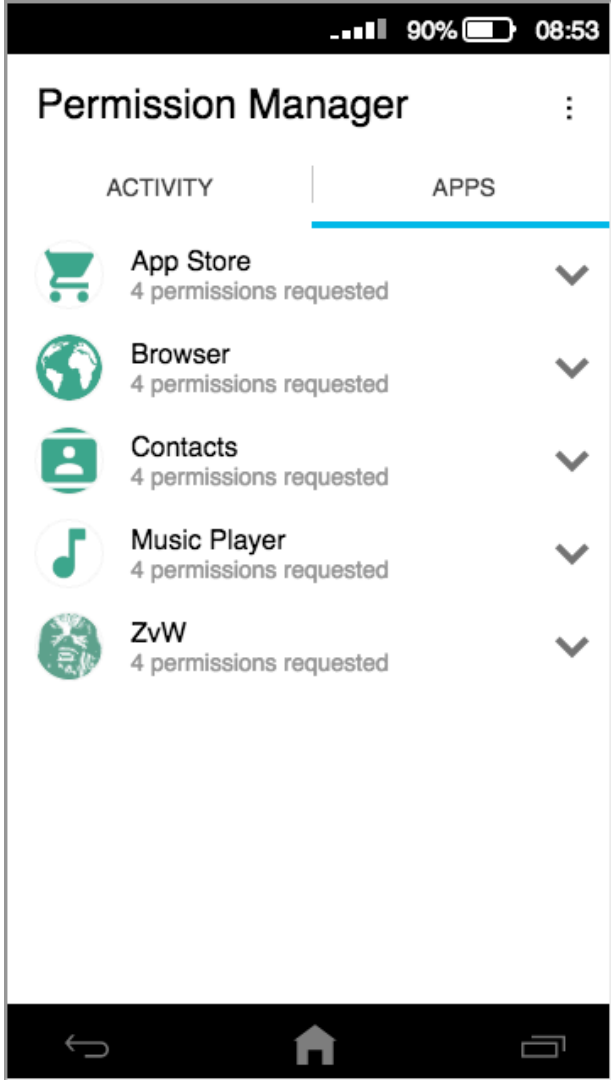
does it help users regulate access based on context?

C. Thompson, M. Johnson, S. Egelman, D. Wagner, and J. King. *When It's Better to Ask Forgiveness than Get Permission: Designing Usable Auditing Mechanisms for Mobile Permissions.* In Proceedings of the 2013 Symposium on Usable Privacy and Security (SOUPS '13).

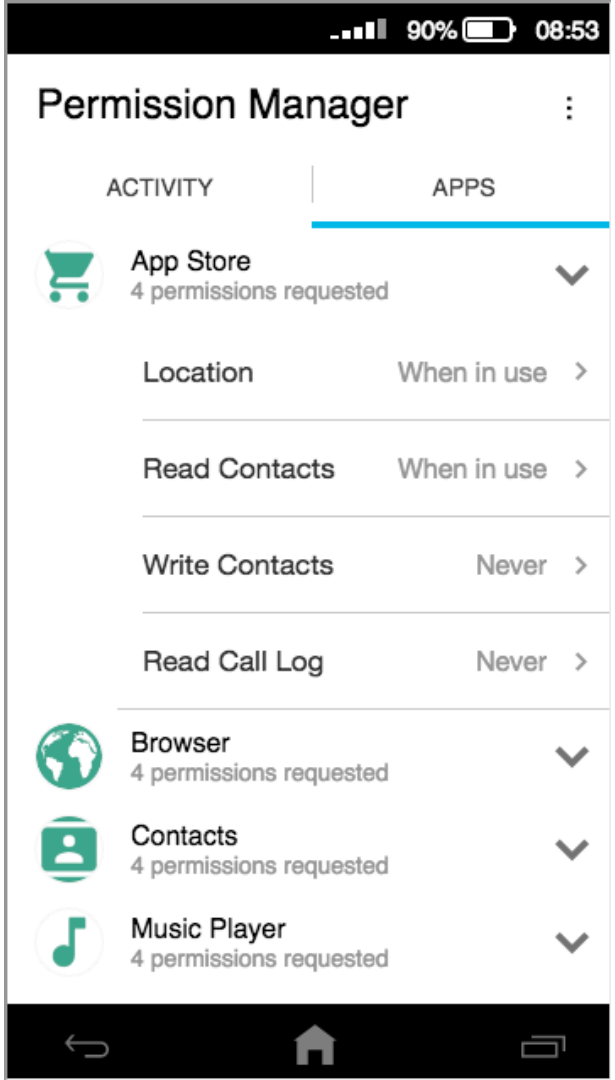
TurtleGuard



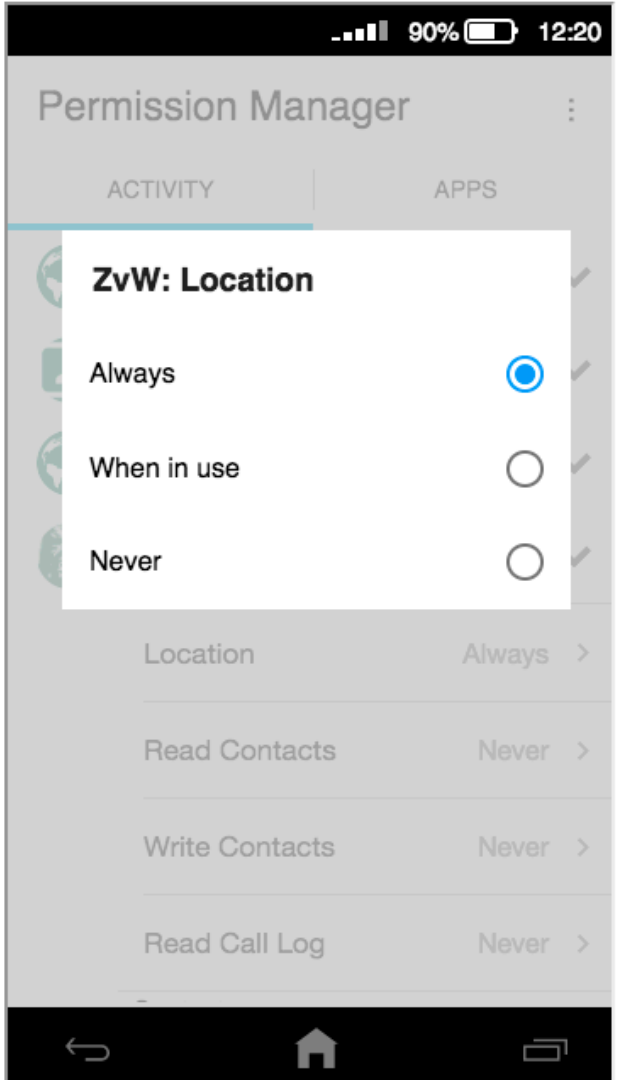
TurtleGuard



TurtleGuard



TurtleGuard



dashboard user study

functioning prototype implemented in HTML5:

- control (Android M settings panel)
- study conducted online (n=400)

tasks designed to test:

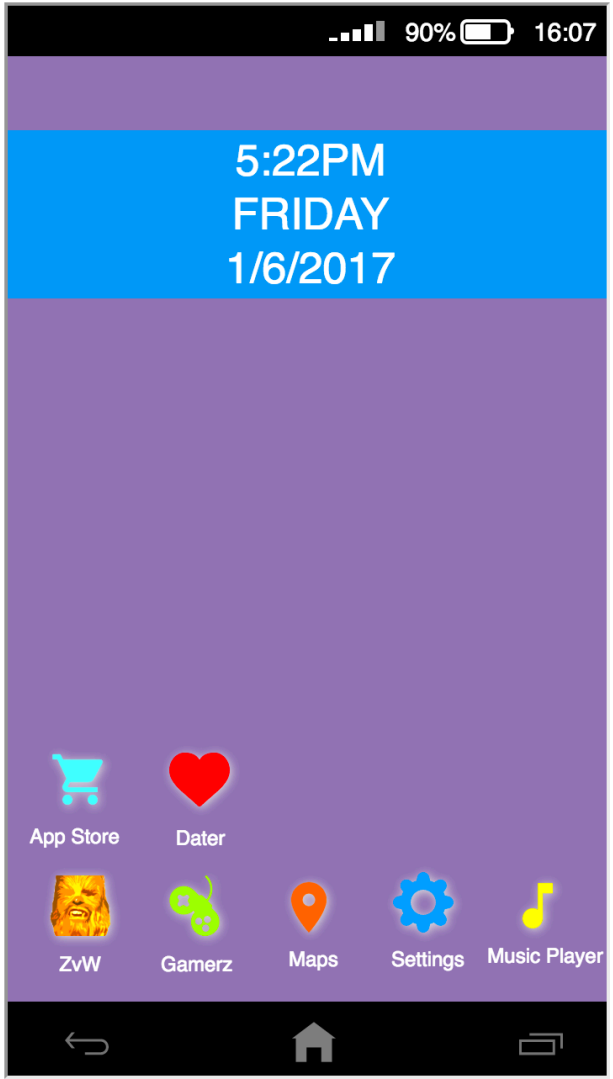
- understanding resource usage
- fixing misaligned settings

task 1

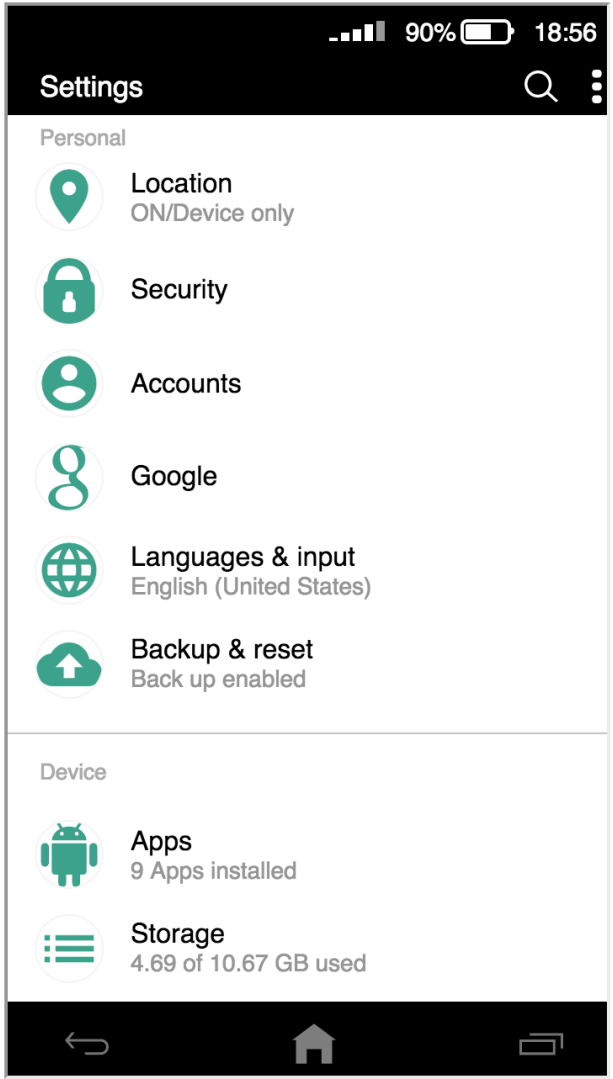
what are the two most recent apps that accessed the device's location?

- open-ended response

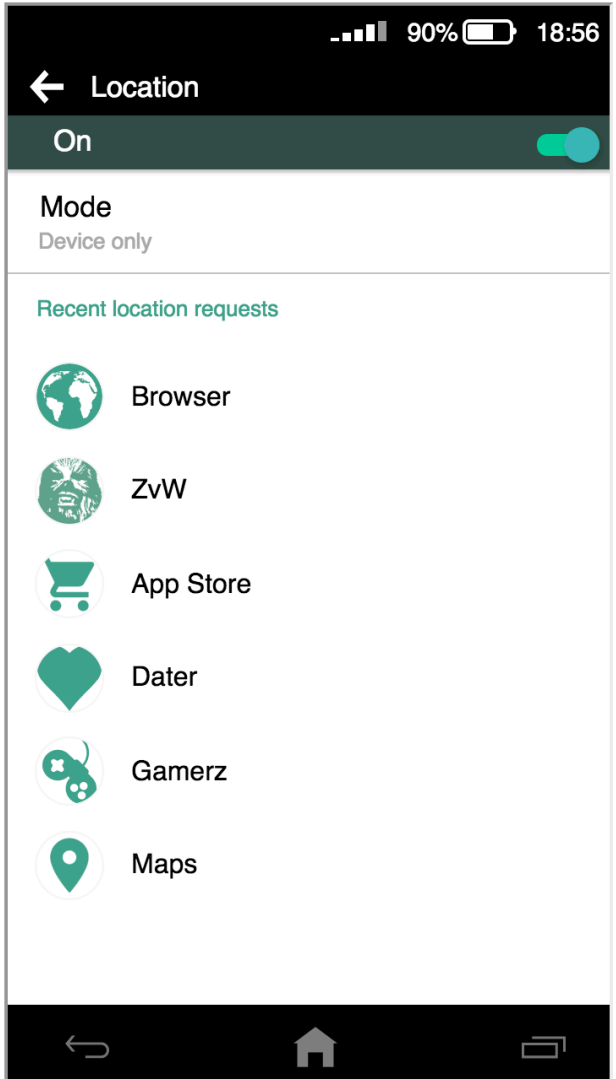
task 1: control



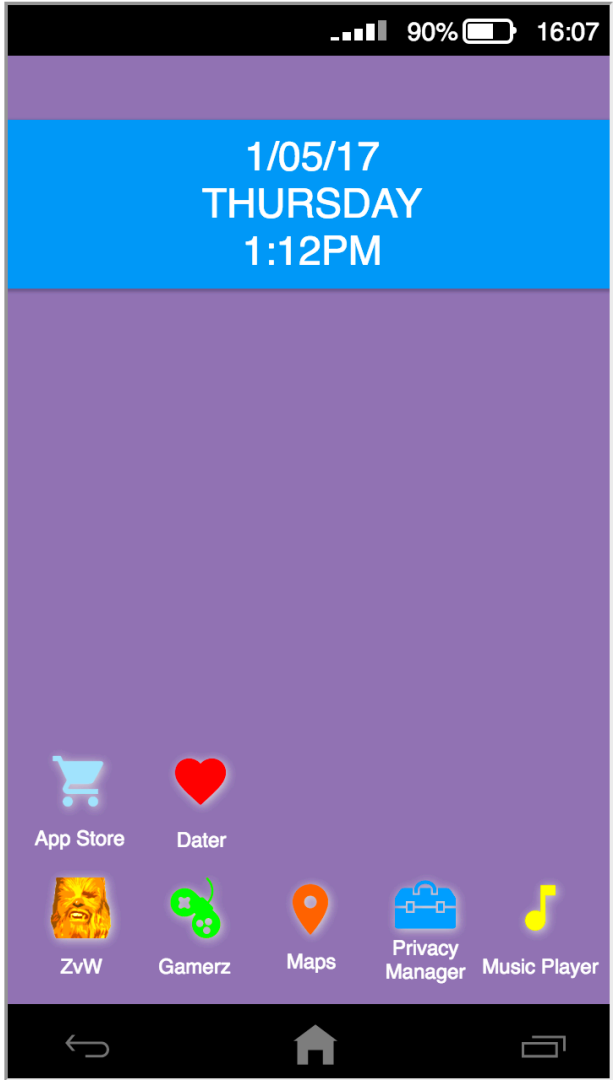
task 1: control



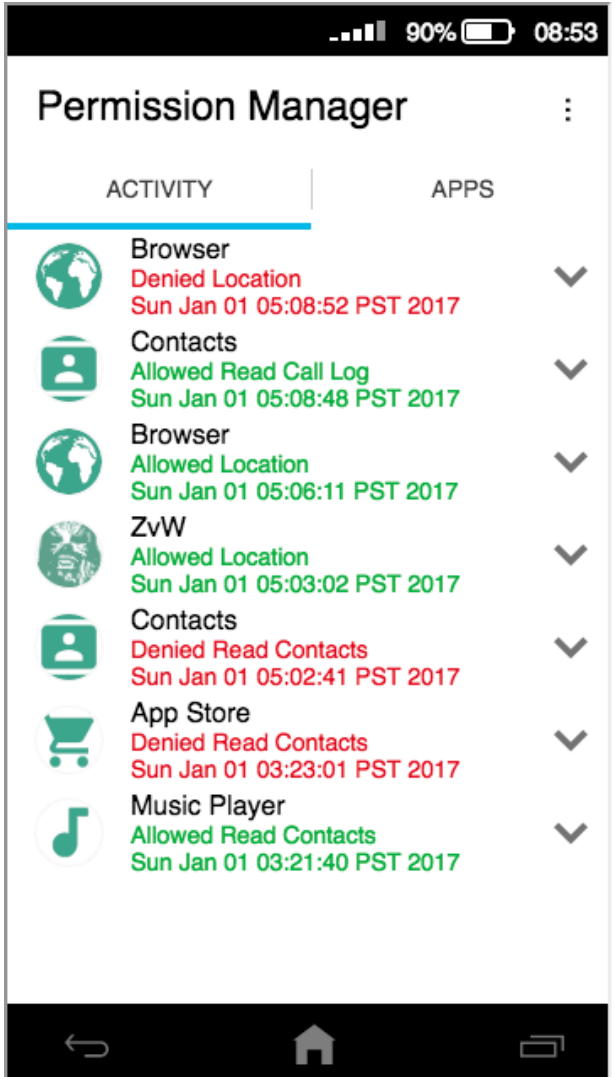
task 1: control



task 1: TurtleGuard



task 1: TurtleGuard



task 1

results:

- control: 84% correct (167/198)
- TurtleGuard: 68% correct (132/194)

observations:

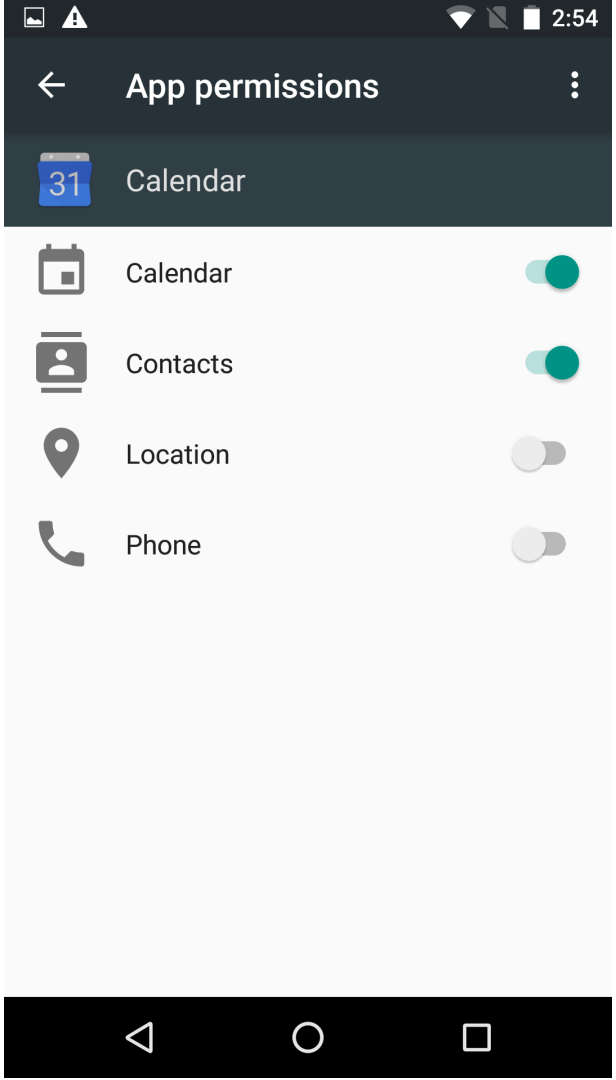
- confusion from presenting all data types together
- a quarter never opened TurtleGuard

task 2

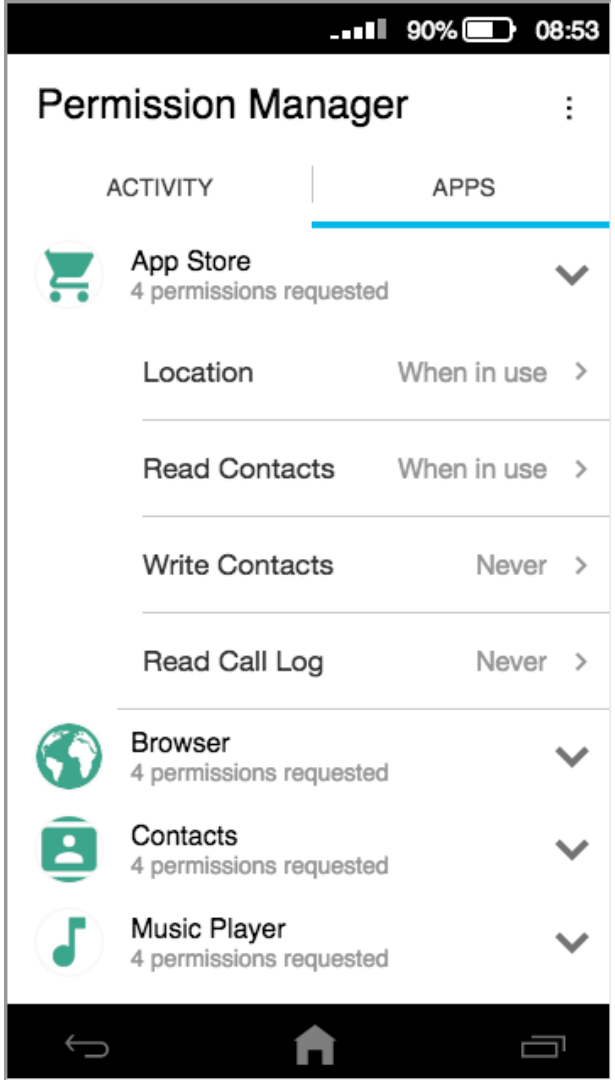
currently, which of the following data types can be accessed by the ZvW app?

- multiple choice

task 2: control



task 2: TurtleGuard



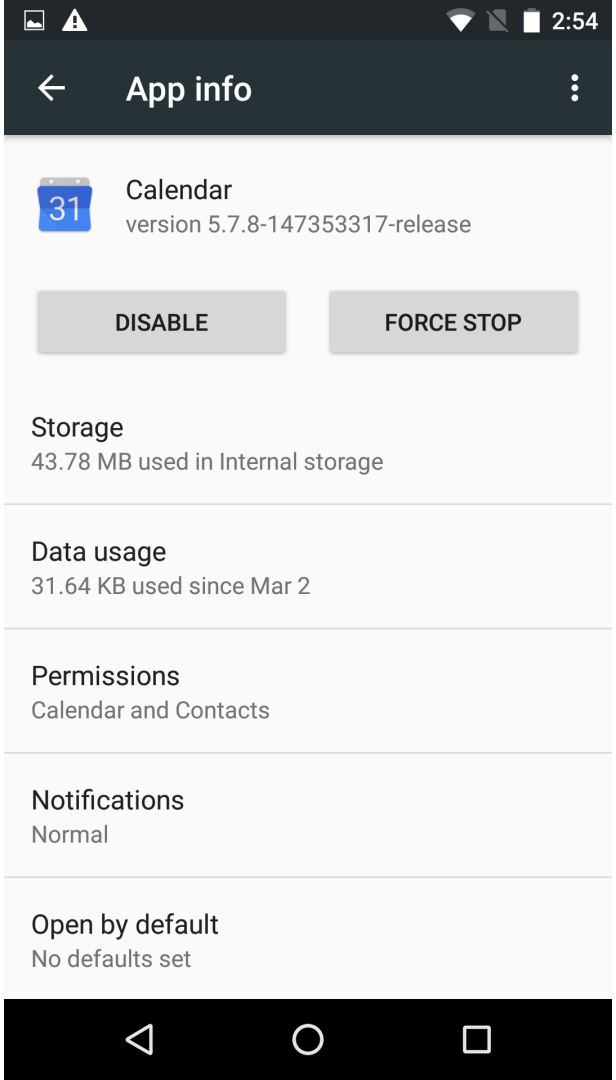
task 2

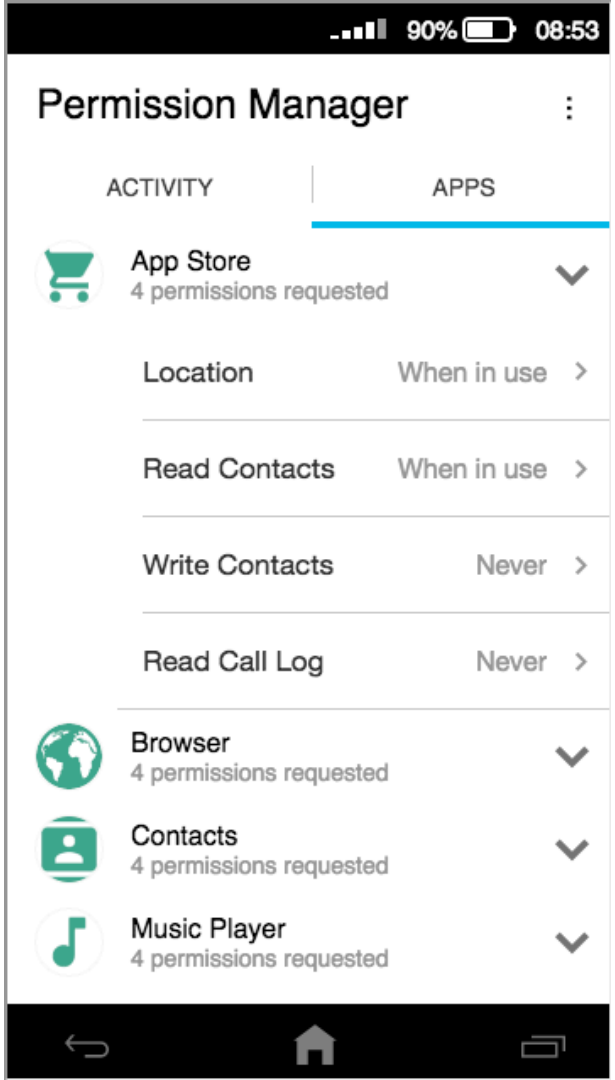
results:

- control: 70% correct (140/198)
- TurtleGuard: 59% correct (116/194)

observations:

- several confounding factors


2:54
App info
Calendar
version 5.7.8-147353317-release
DISABLE
FORCE STOP
Storage
43.78 MB used in Internal storage
Data usage
31.64 KB used since Mar 2
Permissions
Calendar and Contacts
Notifications
Normal
Open by default
No defaults set


90%
08:53
Permission Manager
ACTIVITY
APPS
App Store
4 permissions requested
Location
When in use
Read Contacts
When in use
Write Contacts
Never
Read Call Log
Never
Browser
4 permissions requested
Contacts
4 permissions requested
Music Player
4 permissions requested

tasks 3 & 4

is the ZvW app able to access location data even when it is not actively being used?

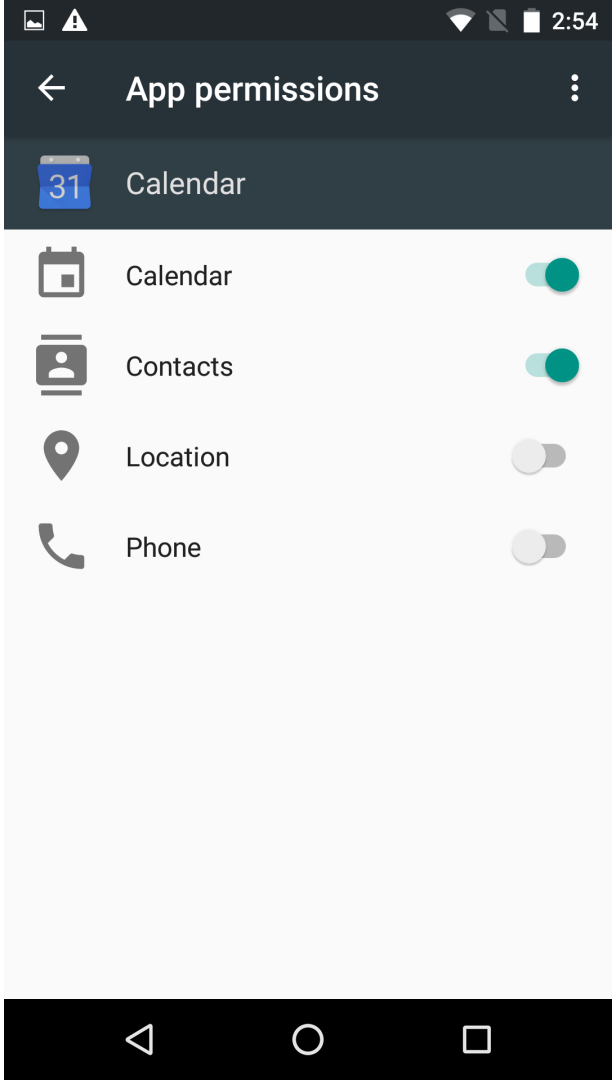
- multiple choice

prevent it from doing so…or explain whether it is even possible

- open-ended response

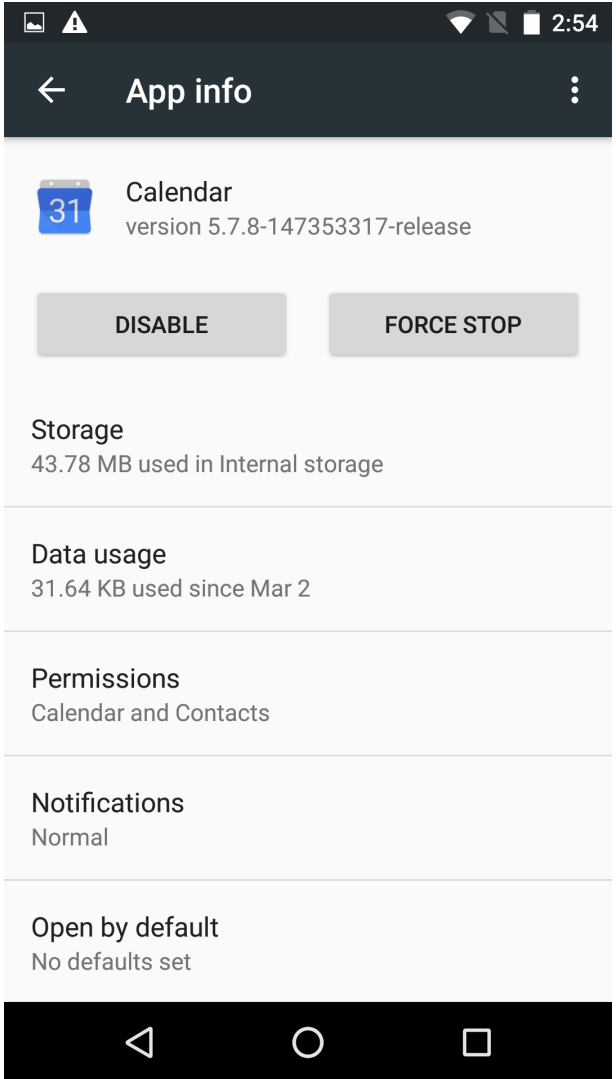
tasks 3 & 4: control

- answering question relies on knowledge of Android!
- not possible to regulate foreground vs. background data access!

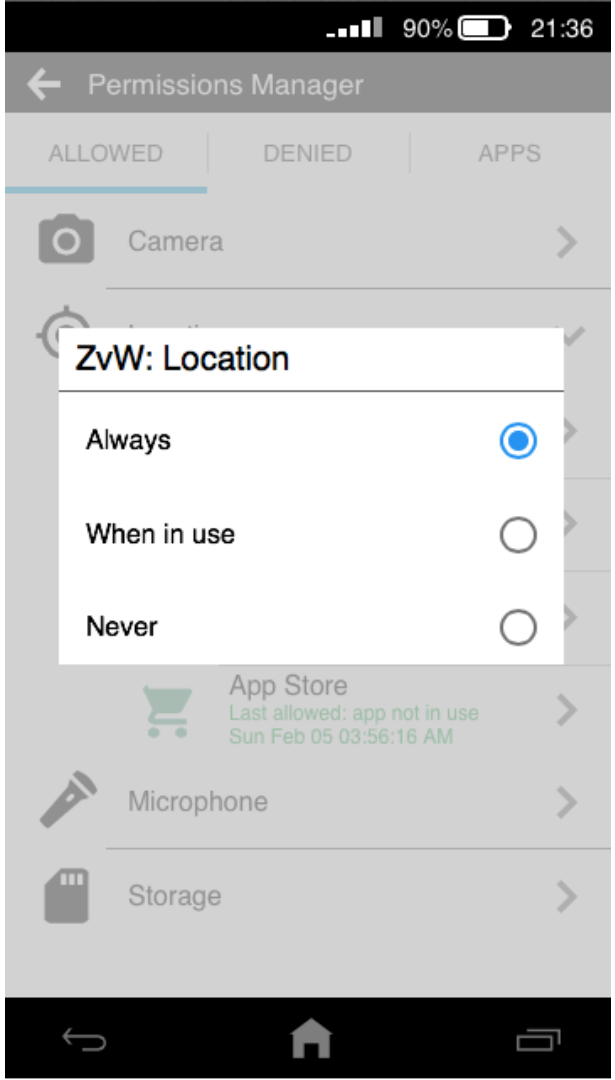


tasks 3 & 4: control

- answering question relies on knowledge of Android!
- not possible to regulate foreground vs. background data access!



tasks 3 & 4: TurtleGuard



tasks 3 & 4

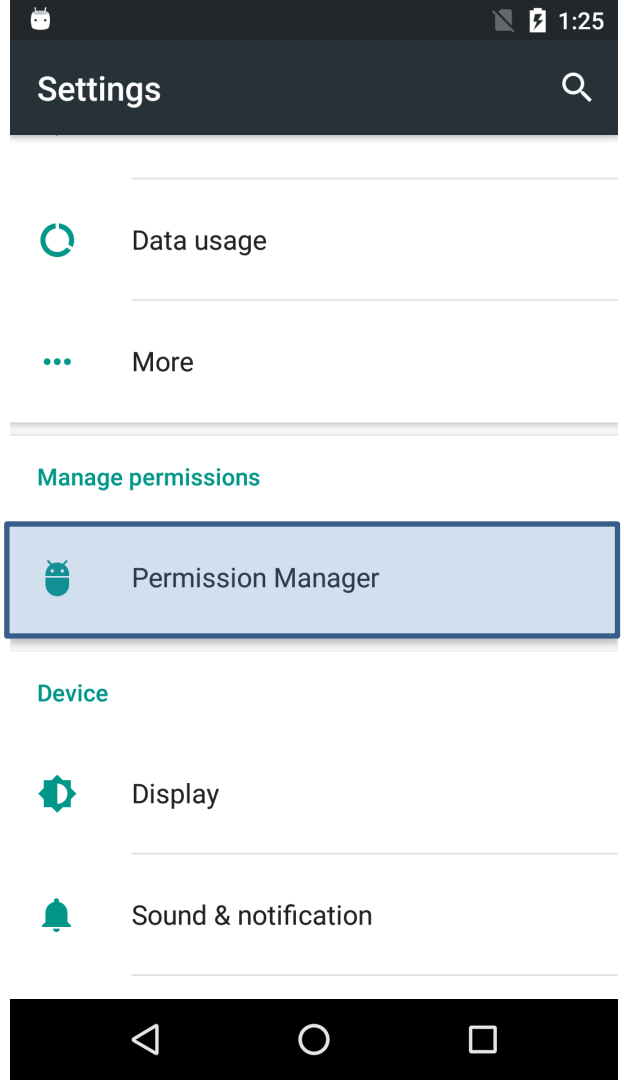
results:

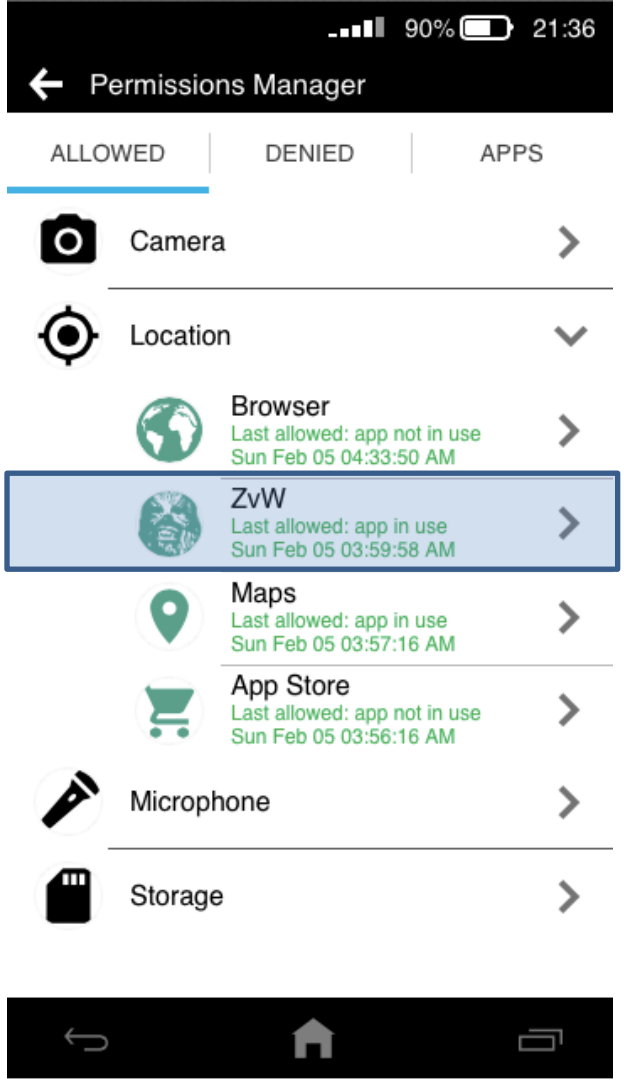
- control:
  - 43% understood background access would occur
  - 23% correctly understood they could not regulate it
- TurtleGuard:
  - 78% understood background access would occur
  - 75% were able to limit it

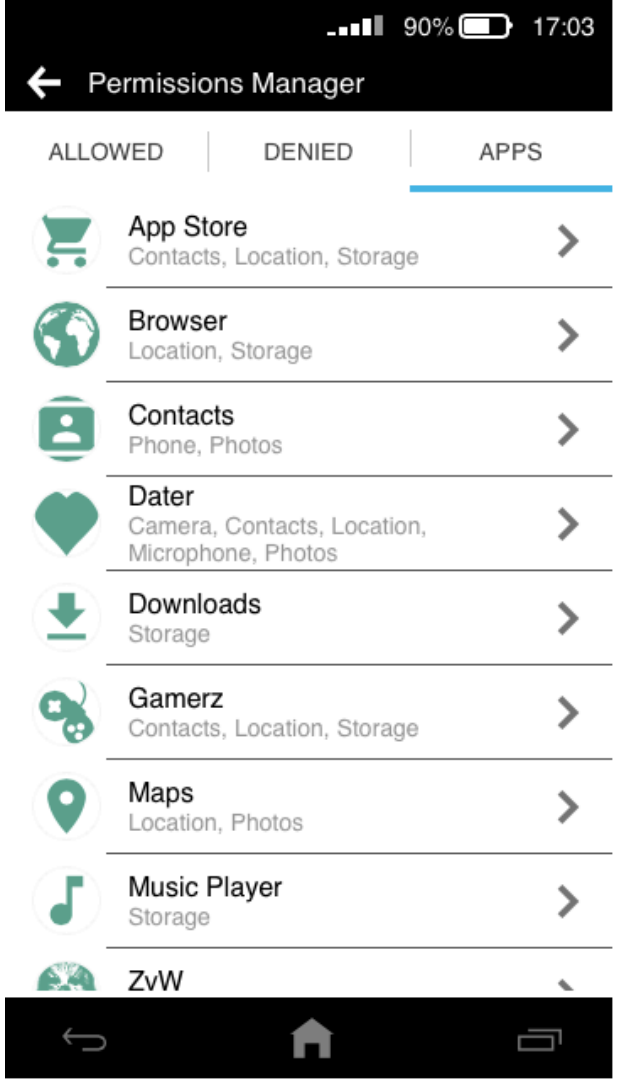
observations:

- strong effects ($\Phi_{task\ 3}$=0.36, $\Phi_{task\ 4}$=0.51)

ITERATIVE DESIGN


1:25
Settings
Data usage
More
Manage permissions
Permission Manager
Device
Display
Sound & notification


90%
21:36
Permissions Manager
ALLOWED
DENIED
APPS
Camera
Location
Browser
Last allowed: app not in use
Sun Feb 05 04:33:50 AM
ZvW
Last allowed: app in use
Sun Feb 05 03:59:58 AM
Maps
Last allowed: app in use
Sun Feb 05 03:57:16 AM
App Store
Last allowed: app not in use
Sun Feb 05 03:56:16 AM
Microphone
Storage


90%
17:03
Permissions Manager
ALLOWED
DENIED
APPS
App Store
Contacts, Location, Storage
Browser
Location, Storage
Contacts
Phone, Photos
Dater
Camera, Contacts, Location,
Microphone, Photos
Downloads
Storage
Gamerz
Contacts, Location, Storage
Maps
Location, Photos
Music Player
Storage
ZvW

VALIDATION STUDY

methodology

repeat of pilot study

- same 4 tasks

new Mechanical Turk participants (n=298) compared with Prolific Academic sample (n=300)

- no differences in behavior

validation study results

task 1: understanding recent location access

- control: 83% correct (of 287)
- TurtleGuard: 83% correct (of 293)

task 2: finding granted permissions

- control: 77% correct (of 287)
- TurtleGuard: 81% correct (of 293)

validation study results

task 3: understanding privacy settings (background access):

- control: 38% correct (of 287)
- TurtleGuard: 79% correct (of 293)
- medium-to-large effect size: ϕ=0.41

task 4: changing privacy settings (background access):

- control: 28% said it was impossible (of 287)
- TurtleGuard: 77% correctly did it (of 293)
- large effect size: ϕ=0.49

conclusions

demonstrated how to use iterative user-centered design to construct a new interface for managing app permissions:

- without prior training, performs as well as the permissions interfaces users are accustomed to
- performs significantly better at communicating foreground vs. background data access

NEXT STEPS

validation field study

we have a working prototype…

…how will real users use it?

will users make the same decisions when permission are actually denied?

will they rectify errors with the dashboard?

validation field study

methodology

- recruit 40 local Android users
- use our phones as their own for a week
- measure decision-making and interactions
- post-study interviews/tasks

questions?