CLTC Center for Long-Term Cybersecurity
UC Berkeley

Berkeley UNIVERSITY OF CALIFORNIA

ICSI INTERNATIONAL COMPUTER SCIENCE INSTITUTE

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

# Evaluating and Redefining Smartphone Permissions with Contextualized Justifications for Mobile Augmented Reality Apps

David Harborth and Alisa Frik

USENIX Symposium on Usable Privacy and Security (SOUPS 2021)

10 August 2021

# Agenda

1. Motivation and Background
2. Research Questions
3. Method
4. Results
5. Discussion

# Motivation and Background

- Augmented reality (AR) “[...] combines real and virtual objects in a real environment; runs interactively, and in real time; and registers (aligns) real and virtual objects with each other" [Azuma et al. 2001, p. 34]

- AR as the next “big technology” [Business Insider Intelligence 2016, Cook 2016]
- 83.1 million users in the US in 2020 [Petrock 2020]

- Our work focuses on the end users of mobile AR technologies (MAR)

# Privacy in Mobile AR

Amplified risks and concerns:

- More sensors and associated data required due to context-dependency for realistic experience
- Potential for realistic deceptive malicious interventions
- Even more limited transparency about data practices

→ Smartphone permissions are an integral part for providing information about apps' data collection practices

- Existing permission systems are criticized for inattention to context [Kelley et al. 2012, Wei et al. 2012, Wijesekera et al. 2015],

# Research Questions

RQ1: How does information provided in smartphone permissions affect users' understanding of what resources and data are accessed by an MAR app? And what are users' expectations about the impact of these permissions on the app's performance?

RQ2: How does information provided in permissions affect users' privacy concerns regarding MAR apps?

RQ3: How do the justifications for requesting smartphone permissions affect users' choices regarding whether to grant such permissions and whether to download an MAR app?

RQ4: How can the transparency of smartphone permissions in MAR apps be improved?

# Method – Research Design

- Study 1 (N=292), Study 2 (N=289)
- Between-subjects design
  - Control (permission labels only)
  - vs Non-Contextualized Justifications (NCJ)
  - vs Contextualized Justifications (CJ)

- Willingness to grant permission
- Privacy concerns
- Informativeness of the permissions
- App download intention (Study 2)
- Open-text answers about additional information required for better understanding of the app's data practices (Study 1)

# Method – Permission Set

- 7 existing permissions and 9 new ones reflecting resources needed by MAR apps

| Existing permissions | Newly introduced permissions |
|---|---|
| Storage / Photos / Media Library | Accelerometer |
| Contacts | Gyroscope |
| Network / Internet Access | Magnetometer |
| Microphone | LiDAR Scanner |
| Camera | Geometry Tracking |
| Location Services | Raw Camera Output |
| Notifications | Object Recognition |
| | Face Recognition |
| | Speech Recognition |

# Results: Contextualized Justifications

Contextualized justifications about data use (descriptions tailored to the app's context)

- Improve general understanding of app's data practices and the perceived permission informativeness
- Mitigate privacy concerns (in Study 2)

# Results: No Justifications

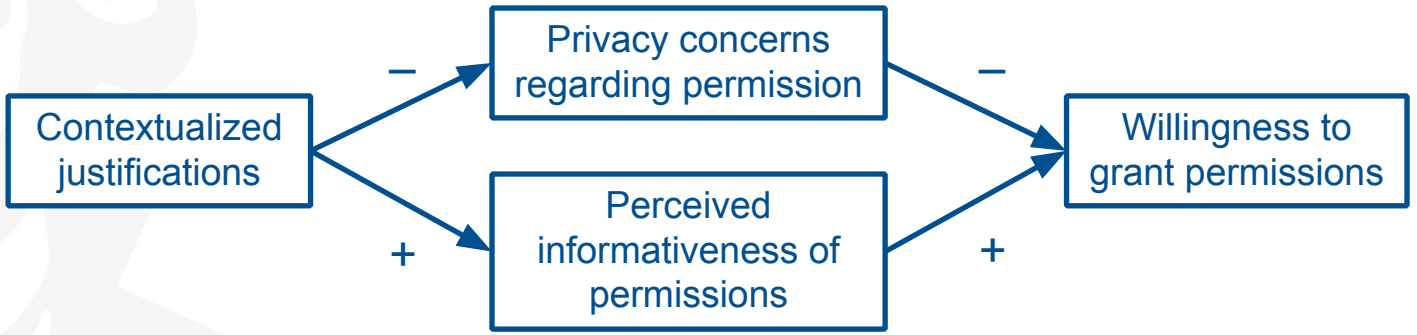
In the conditions without justifications requested:

- More clarifications about what data is collected by the app
- How data is used
- Whether it is possible to decline the permission and how it would affect the app's performance

# Results: Mediation Effects

Contextualized Justifications do not directly affect the willingness to grant the permissions or download the app, but there is a mediating effect:

- Privacy concerns negatively affect the willingness to grant permissions and
- Perceived informativeness of the permissions about app's data practices (transparency) positively affect willingness to grant permissions
- Improved transparency and lower perceived privacy danger increase the willingness to grant permissions



# Recommendations

Improve MAR app permission transparency:

- Add permissions about new sensors and data processings that are perceived as dangerous (e.g. face
  and speech recognition)
- Introduce contextualized justifications and show when functionalities or data are accessed
- Test linguistic complexity of justifications and explanations
- Use short descriptions of novel sensors and functions
- Improve visual appearance by grouping permissions (e.g., by use), expandable text boxes (avoiding fatigue)
- Indicate whether permission can be denied

# Key take-aways:

Key take-aways:

- Justifications are useful for creating transparency, but they need to be meaningful, easy to understand and tailored to the context of the app
- New permissions that raise significant concerns among participants should be added
- Knowledge-concern gap for MAR apps: users need to be informed about technical possibilities to exploit the variety of sensors (clarifications and justifications one step towards addressing this)

Future Work:

- Cross-country comparison of users' perceptions and understanding of MAR apps
- Field experiments with other app categories to evaluate ecological validity

# REFERENCES


- Azuma, R. T., Baillot, Y., Feiner, S., Julier, S., Behringer, R., & Macintyre, B. (2001). Recent Advances in Augmented Reality. *IEEE Computer Graphics And Applications*, 21(6), 34–47.
- Business Insider Intelligence (2016). The virtual and augmented reality market will reach $162 billion by 2020. URL: http://www.businessinsider.de/virtual-and-augmented-reality-markets-will-reach-162-billion-by-2020-2016-8?r=US&IR=T.
- Cook, T. (2016). Apple CEO Tim Cook thinks augmented reality will be as important as “eating three meals a day.” Retrieved January 27, 2017, from http://www.businessinsider.com/apple-ceo-tim-cook-explains-augmented-reality-2016-10?r=US&IR=T.
- Patrick G. Kelley, Sunny Consolvo, Lorrie F. Cranor, Jaeyeon Jung, Norman Sadeh, and David Wetherall. (2012). A conundrum of permissions: installing applications on an android smartphone. In *Proceedings of the 26th International Conference on Fin. Cryptography and Data Security*, 68–79.
- Petrock, V. (2020). US Virtual and Augmented Reality Users 2020. URL: https://www.emarketer.com/content/us-virtual-and-augmented-reality-users-2020.
- Python Software Foundation. textstat 0.7.0. https://pypi.org/project/textstat/, 2021.
- Xuetao Wei, Lorenzo Gomez, Iulian Neamtiu, and Michalis Faloutsos. (2012). Permission evolution in the android ecosystem. In *Proceedings of the 28th Annual Computer Security Applications Conference*, 31–40.
- Wijesekera, P., Baokar, A., Hosseini, A., Egelman, S., Wagner, D., & Beznosov, K. (2015). Android Permissions Remystified: A Field Study on Contextual Integrity. Proceedings of the 24th USENIX Security Symposium, 499–514. http://arxiv.org/abs/1504.03747

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

THANKS FOR YOUR ATTENTION!

Please contact me for follow-up questions:

david.harborth@m-chair.de