Approximate vs Precise: An Experiment in What Impacts User Choice When Apps Request Location Access

Alex Berke
Google
USA
aberke@google.org

Jessica Johnson
Google
USA
johnsonjj@google.com

Abstract

User location data is highly sensitive, yet commonly requested by mobile apps for both core functionality and monetization. To improve user privacy, the major mobile platforms, Android and iOS, made changes so that when apps request precise location access, users can choose to share only their approximate location. However, the platforms have diverging interfaces: Android offers a side-by-side choice and iOS offers a corner toggle. This study evaluates which factors impact users' choices when apps request location access via a randomized controlled experiment with 2579 US Android users. We tested the impact of app type, whether a reason for the request was provided, and the quality and content of the reason, including monetization. We do not find the reasons have an effect. Instead, we find users' choices are impacted by app type and user demographics. We find that when users are given a side-by-side choice to allow approximate versus precise location access, they make reasonable choices. Of users who allowed access, the vast majority (90.7%) chose precise for a rideshare app versus the majority (71.3%) chose approximate for a local news app. Concerningly, the majority also allowed location access to a wallpaper app, and older users were significantly more likely to allow apps precise location access. We conclude by discussing implications for app platforms and future work.

CCS Concepts

• **Human-centered computing** → **User studies**; • **Security and privacy** → **Usability in security and privacy**.

Keywords

Randomized controlled experiment, user study, quantitative analysis, location data, privacy

ACM Reference Format:
Alex Berke and Jessica Johnson. 2026. Approximate vs Precise: An Experiment in What Impacts User Choice When Apps Request Location Access. In *Extended Abstracts of the 2026 CHI Conference on Human Factors in Computing Systems (CHI EA '26), April 13–17, 2026, Barcelona, Spain.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3772363.3798592

CHI EA '26, Barcelona, Spain

ACM ISBN 979-8-4007-2281-3/2026/04
https://doi.org/10.1145/3772363.3798592

1 Introduction

User location data is highly sensitive yet is one of the most commonly requested resources by mobile applications [11, 35]. Apps often request users' locations for reasons core to the app's functionality, but also often for analytics and monetization [27], and reasons that might not be clear to users.

The high value and sensitive nature of user location data presents privacy risks. There is a multibillion dollar market for location data [20, 25] and previous work has shown how commonly used mobile apps disclose users' location data to ad servers and other third parties without users' informed consent [15], both deliberately and inadvertently [24]. Moreover, recent high-profile data leaks and reporting have shown that this user location data ends up with data brokers and is available for sale [12, 13, 28]. This data can expose sensitive information about users such as their home, work or worship locations, health status, or social and political ties [24].

To help address these risks, the major mobile app platforms, Android and iOS, require apps to request permission from users before accessing their locations, in runtime dialogs [2, 8]. Given that users' precise location is more sensitive than their general area, both platforms updated their location request dialogs to allow users to choose to share only their approximate location when apps request their precise location. This privacy enhancement was introduced in 2020 for iOS 14+ [6] and 2021 for Android 12+ [5]. With these changes relatively new, there is a lack of research on how users make decisions to grant precise versus approximate location access. In this work we address that gap.

Furthermore, although Android and iOS both now allow users to share only their approximate location, their interfaces that enable that option are different (see examples in Appendix Figure 4). In both interfaces, precise location is the default. In Android, the location request dialog presents users with a side-by-side choice for sharing their precise versus approximate location, while in iOS the option to share approximate instead of precise location is in a corner toggle. Yet a side-by-side choice may lead to degraded functionality for apps that rely on precise location when users instead choose approximate, which could occur when users do not understand the implications of choosing approximate versus precise location. In this study we evaluate whether users understand the difference and whether they make reasonable selections when given a side-by-side choice.

Our study is designed around the following research questions:

- RQ1: Do users understand when to allow apps to access their precise versus approximate location?
- RQ2: How does whether an app provides a reason for requesting location access, or the reason itself, impact user choice?
- RQ3: How does the type of app impact user choice?
- RQ4: Is there a relationship between users' demographics and location sharing choices?

We answer these questions by conducting a randomized controlled experiment with over 2500 US Android users, where different participants see different versions of location access request dialogs for various apps. We test 3 different types of common apps that vary in how they need location for core functionality: (1) A wallpaper app (no need for location), (2) a local news app (approximate location) and (3) a ride share app (precise location). For each app, we test 4 different versions of the requests: (A) a version where the app provides no reason for the request, (B) a version where the app provides a high quality reason that does not mention ads, (C) a low quality, uninformative reason, and (D) a reason that mentions using location for ads and monetization.

We do not find the request reasons played a significant role in users' choices. Instead, we find choices are driven by the app type and user demographics. Users were significantly more likely to grant location access to the local news and rideshare apps versus the wallpaper app, and their choices demonstrated an understanding of when to allow precise versus approximate location. Of users who granted location access, the vast majority (90.7%) chose precise for the rideshare app and also the majority (71.3%) chose approximate for the local news app. Yet concerningly, many users also granted location access to the wallpaper app, including precise location. Together, our results suggest users can make reasonable selections between precise versus approximate location access when given a clear choice, but privacy risks remain for many users who allow unnecessary location access. Considering who these users may be, we find that older users are significantly more likely to allow precise location access. These findings have important implications for app platforms as they consider further changes to improve user location privacy; we conclude by discussing these implications and future work.

2 Background and related work

To the best of our knowledge, this is the first study to experimentally investigate how users make choices when allowing precise versus approximate location access to mobile apps.

An early 2014 study, with 106 online participants, found Android users could differentiate between the two location permission options and interpreted "precise location" as exact and "approximate location" as a general area [19]. However, this study was carried out years before users had an option to choose between precise versus approximate location in request dialogs in either Android or iOS, and unlike our study, it did not test how users made choices when presented with request dialogs. A more recent analysis investigated how some of the top Android and iOS apps behave when users allow only approximate, rather than precise, location access [22]. It found that for many top apps, functionalities were removed or degraded when only approximate location was allowed, implying it may be important for users to make appropriate selections for optimal user experiences. However, their analysis was limited to testing apps rather than user behavior, which our study provides.

With respect to why location data is important to protect, other analyses of popular mobile apps have found that many share location data with advertisers and other third parties without users' informed consent [15, 24], or in ways that transgress the expectations of users [21, 33], violating the concept of contextual integrity, which conceives privacy as the appropriate flow of information, given the context [31]. These include analysis of a top ride share app [21], and analysis of popular weather apps, which found many of the apps collected location data in ways that violated their own policies, and many did not identify the third-party recipients of the data they collected [33].

Analysis has also identified ads and analytics as the top two reasons for data sharing [27] and a prior study with over 2000 US users showed some (4%) were willing to share their precise, current location data with online advertisers, with more (over 20%) willing to share their approximate location (e.g. zipcode) [29]. We incorporate these findings into our experiment design by testing how users behave when apps state their use of location data includes advertising.

Location data is one of the many sensitive resources that Android and iOS protect with a permissions system [3, 7], requiring app developers to prompt users with a request to access their data (e.g. location) before the app can use it. These permission systems have evolved throughout the years and researchers have studied their impact on both apps and users. For example, in early versions of Android all permissions were requested at installation time. Studies then showed a prevalent problem where many apps were overprivileged (requested more permissions than necessary) [16] and that these install-time requests led to low attention and comprehension rates by users [18, 26]. Researchers thus advocated for a more contextualized permission model [17, 38] and Android version 6.0 introduced runtime permissions [4], which were already present in iOS, where users see permission requests when a resource is first needed. These runtime permission systems allow apps to provide reason strings, specifying why the requested resource is needed [3, 7].

Our study builds on a 2014 investigation of how including reasons in permission requests impacts grant rates. This prior study was conducted soon after reason strings were introduced in iOS, yet before users had an option to allow approximate versus precise location [36]. It was conducted online with 772 smartphone users and tested requests for six different resources, including geolocation. The researchers found that overall, the rate at which users granted permission requests increased when reasons were present, compared to a control without reason strings. Surprisingly, they observed this was

the case regardless of the reasons' contents. Similarly, we also test the impact of providing reasons in permission requests, with varying reasons and a control. However, we focus on how users choose between approximate versus precise location access, while also testing how different types of apps, with varying location needs, impact choice.

More recent work has also studied users' relationships to permission requests, with a 2023 study finding users are overall worried about permission requests, and see the location permission as particularly sensitive, with privacy ramifications [35]. These studies have also found that the information provided in request dialogs is insufficient for users to understand the scope of how their data will be accessed [11, 34], yet users who better understand permissions tend to be more conservative in granting them [34]. A 2017 study of Android users' decisions to grant versus deny permission requests followed their real world app use [11]. It found that the main reasons for denying location permission requests were users' belief that the app would still work without the permission, or that they could change their mind later, or they did not trust the app with the information. They also found important demographic differences when comparing age and gender, where women denied permissions twice as often as men. Other studies focused on location privacy, outside of the permission request context, have similarly found differences across gender and age groups, where females consistently express greater concern around location sharing [1, 10]. We build on these findings by also testing how location preferences differ by age and gender.

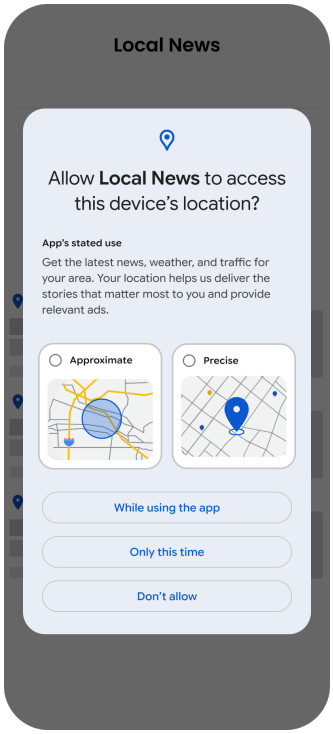


Figure 1: Example of a location access request dialog shown to participants in our experiment, corresponding to 2.D in Table 1.

3 User study

We conducted a randomized controlled experiment in order to test which factors impact users' choices when allowing apps to access their approximate versus precise locations. Our experiment focuses on Android, which provides a clear side-by-side choice between approximate and precise location access.

3.1 Experiment design

We designed our experiment to test how different types of apps (with different needs for location), and different reasons the apps provide for requesting location access, impact user choice. Table 1 summarizes our experiment design, showing the apps and reasons tested. For each app and request reason, we showed participants a corresponding location request dialog, and asked participants to make their access choices. An example is shown in Figure 1. All request dialog images corresponding to Table 1 are shown in Appendix Table 3.

3 app types. We tested (1) a wallpaper app, (2) a local news app, and (3) a ride share app. We chose these three types of apps because (a) we expect most users to be familiar with them and (b) their core functionalities have varying requirements for location access, which should be clear to a familiar user: (1) a wallpaper app does not need location access for core functionality, while (2) approximate location access improves functionality for a local news app, but precise location is not necessary. Finally, (3) precise location access improves functionality for a ride share app.

4 experiment groups. For each app, we tested four different request reasons. (A) A control where no reason was provided, (B) a "high quality" reason, (C) a "low quality", uninformative reason which added no additional information for the user to understand the reason for the request, and (D) a reason that mentioned the use of location for ads and monetization, following text similar to the "high quality" reason.

Participants were randomly assigned, with equal probability, to one of four experiment groups, which included a control group. The control group was not shown any reasons in the request dialogs (A). Experiment group 1 was shown only "high quality" reasons (B). We set up the experiment to avoid showing any participant only low quality or ads related reasons. For Experiment groups 2 and 3, for each app, participants had a 50% random chance of seeing either the high quality reason (B) or the experiment group specific reason: "low quality" for group 2 (C), or ads related for group 3 (D).

3.2 Survey

Our survey instrument was implemented via Qualtrics. The full survey text is provided via the Appendix.

App		Permission request reason shown by experiment group			
Type	Note	A. Control	B. High quality	C. Low quality	D. Mentions ads
(1) Wallpaper	Location not needed for core functionality.	–	Your location will be used to help WallpaperApp improve our service, so we can provide you with a better experience.	Your location is needed for app functionality.	Your location will be used to help WallpaperApp improve our service to give you a better experience and optimize our ads and marketing strategies.
(2) Local news	Only approximate location needed for core functionality.	–	Get the latest news, weather, and traffic for your area. Your location helps us deliver the stories that matter most to you.	Your location is needed for app functionality.	Get the latest news, weather, and traffic for your area. Your location helps us deliver the stories that matter most to you and provide relevant ads.
(3) Ride share	Precise location improves core functionality.	–	To help get you to your destination, RideShare uses your location to find drivers nearby, improve pickups, support, and more.	Your location is needed for app functionality.	To help get you to your destination, RideShare uses your location to find drivers nearby, improve pickups, and support our advertising programs.

Table 1: Experiment setup with 3 categories of apps and 4 permission request reasons tested for each app.

Upon entering the survey, participants were asked to provide informed consent to have their responses used in a research publication. This was followed by screener questions, confirming they lived in the US and used an Android device as their primary mobile phone. Participants were then asked demographic questions, followed by an attention check.

Participants were then asked to imagine they were using their real Android device for the following questions before proceeding to the experiment. For each of the apps (Wallpaper, Local news, Ride share) participants were shown a location permission request dialog (similar to Figure 1), which differed depending on their experiment group. They were asked to make their permission selection, choosing between "Approximate" and "Precise" and between the options to allow location "While using the app"/"Only this time"/"Don't allow". The permission request dialogs did not have preselected defaults.

After completing the final experiment questions for the ride share app, participants proceeded to an attention check which confirmed they could identify the type of app they were just asked about. Data were discarded for any participants who did not select a ride share app. This was followed by the question: "What reason did the app provide for requesting access to your location?" (The correct response differed by experiment group.) Our analysis uses whether the participant answered this correctly to test the robustness of our results.

4 Participants

We recruited US Android users via Prolific, which is a commonly used crowdsourcing platform to recruit participants for privacy related studies [14]. To avoid response bias, the survey description did not mention privacy. All participants who completed the survey were paid $1.25 USD, which took them 2.3 minutes on average (median). Participants who did not pass the screening exited the survey early and were paid $0.14 for their short time, as recommended by Prolific [32].

Our analysis sample includes 2579 participants who provided informed consent, confirmed they were US Android users and passed both attention checks. Participant demographics are summarized in Table 2. Further participant details, including the number of participants assigned to each experiment group, are provided in the Appendix (C).

	n	%
Total	2579	100
Gender		
Woman	1285	49.7
Man	1250	48.4
Other (Nonbinary or self-describe)	44	1.7
Age in years		
18 - 34	797	30.8
35 - 54	897	34.7
55+	885	34.2
Education level		
No bachelors degree	1305	50.5
Bachelor's degree	953	36.9
Graduate or professional degree	321	12.4

Table 2: Participant demographics.

5 Analysis and results

Results are summarized in Figure 2 and Figure 3, with numerical results in Appendix Tables 6-7. Overall, the majority of participants allowed location access to each of the apps and 42.9%, 16.9%, and 2.4% of participants denied location access to the Wallpaper, Local news, and Ride share apps, respectively.

To evaluate (RQ1) whether users understand when to allow access to precise versus approximate location, we compare

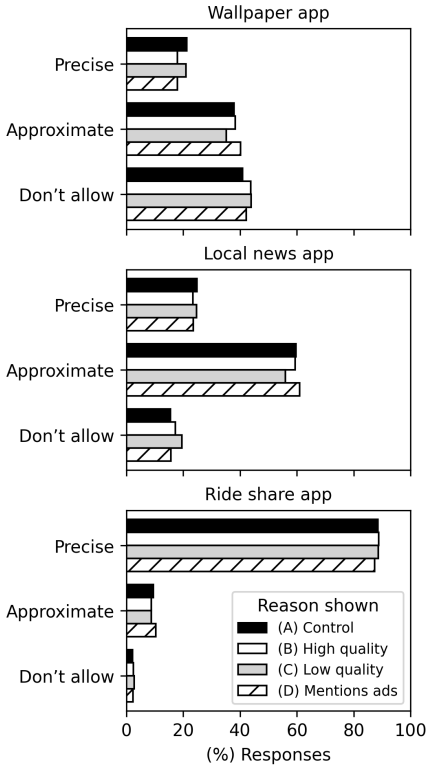


Figure 2: How users chose to allow location access for each app and reason shown.

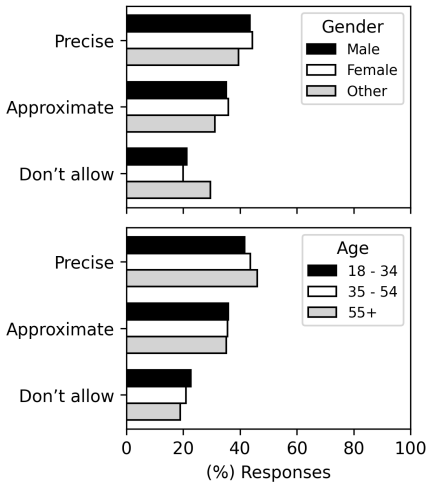


Figure 3: How users chose to allow location access by gender (top) and age (bottom) demographics.

choices for the Local news versus Ride share apps. Among the users who allowed location access, 91% chose precise and 9% chose approximate for the Ride share app, versus 29% chose precise and 71% chose approximate for the Local news app. These results, where the vast majority of users chose precise for the Ride share and approximate for the Local news apps, indicate most users have a good understanding of when to allow approximate versus precise location access and can make appropriate choices when given clear options, without a default.

In order to statistically test which factors impact users' permission choices and evaluate RQ2 - RQ4, we use logistic regression. The independent variables are the app type, the experimental request reason group provided by the app (A-D), and user demographics, where we also test for an interaction effect between app type and reason. First we test for the impact on users' choices to allow location access at all, where the dependent variable is 1 if they allowed access (precise or approximate) and 0 if they chose "Don't allow". Second, we test for the impact on users' choices to allow precise (1) versus approximate (0), where choices for "Don't allow" are excluded. (Detailed regression results are in Appendix Tables 8 - 9.)

We find that the type of app and users' demographics have a significant effect on user choice, but do not find the request reasons had an effect. After participants made their choices for all 3 apps, only the minority (n=829; 32%) were able to correctly identify the last request reason they had seen (for the Ride share app), suggesting most had either not read or not remembered the request reason. For robustness, we test whether the reasons had an effect on the 829 participants who did correctly identify the request reason. We do this by repeating the logistic regression analysis restricted to these participants and the Ride share app responses (which they identified the reason for), and again do not find the reasons had a significant impact (see Appendix Tables 10 - 11).

Compared to the Wallpaper app, participants were more than 3.5x as likely to allow location access to the Local news app and more than 33x as likely for the Ride share app. And among those who allowed location access, participants were less likely to choose approximate location for the Local news app (many of whom chose "Don't allow" for the Wallpaper app) and more likely to choose precise location for the Ride share app.

With respect to demographics, we find participants who self-identified as a gender outside the male/female binary were less likely to allow location access overall. We also find a relationship between age and permission choices. Compared to younger participants (18 - 34 years), older participants (55 years or older) were significantly more likely to allow location access, and among participants who allowed access, older participants were significantly more likely to allow precise location access.

6 Discussion

This work addresses a gap in the literature on how mobile app users allow versus deny location access requests, and an opportunity to improve user location privacy.

Permission requests have changed multiple times over the years, informed by HCI research [11, 17, 18, 26], which this work builds upon to help inform further changes. The more recent change to location permission requests, where users can choose to share their approximate versus precise location, is a step towards improving users' location privacy. However, the platforms differ in how they present the approximate location option to users, which we briefly discuss.

Platforms may prefer to maintain precise location as the default because it enables more optimal functionality for many apps. User experience could be degraded for apps that rely on precise location access [22] if users do not understand when to allow it. A ride share app is one such example. However, our results suggest most users understand when to allow precise location: among our study participants who allowed location access, 91% chose precise and 9% chose approximate for a ride share app, versus 29% chose precise and 71% chose approximate for a local news app. Interestingly, we found users' choices were driven by the type of app and did not find the reasons the apps provided for the requests played a role.

When considering why platforms would make a clear option for approximate location, the foremost reason is to help users reduce the frequency of sharing their precise locations, to reduce their privacy risks. A concerning result from our study is that the majority of users allowed a wallpaper app to access their location, which likely has little use for location beyond monetization. At the same time, we did not find that the app stating it would use their location data for monetization impacted users' choices. This result may be consistent with prior work that showed most permission requests are granted by users, even when users are not comfortable with the choice [11], which could be partly due to habituation [38]. Precise location is more sensitive than approximate location and consumers tend to stick with preselected defaults [23, 37]. Providing approximate location access as a clearer alternative could reduce users' exposure to unnecessary privacy risks, such as when apps that do not require location for core functionality (e.g. wallpaper apps) share and monetize location data. Furthermore, we found that older users are more likely to allow location access overall, and allow precise location, suggesting they could be more exposed to risk. The mobile platforms have used privacy protections as a marketing strategy [30], and further protecting user location privacy could help their pursuit of a competitive advantage. Given that the request reasons did not measurably impact users' location sharing choices in our study, platforms should pursue other means to reduce unnecessary location sharing, such as further highlighting approximate location access as an alternative option, or other updates to the location request options, user interface, or policies.

Future work can build upon this initial study to address its limitations. Our study was limited to US Android users with Android's location request interface, and it only tested three generic types of apps with straightforward location needs. Future work can evaluate how user choices differ across locales, OS, and varying request interfaces, and whether our results extend to other types of apps that have similar location data needs, as well as the impact of users' brand awareness and trust for specific apps. Also, our study raises questions that should be answered. Namely, we did not explicitly ask users why they made the choices they did, which a follow up survey can ask. Furthermore, our experiment presented users with hypothetical choices, whereas previous work studied how Android users make permission decisions using their own devices "in the wild" [11]. Future work can ask users to report on the actual apps they use and the location permissions they have granted, to further our empirical understanding of users' location and privacy choices.

Acknowledgments

We thank the crowdworkers who participated in our study. We also thank May Smith, Aman Jain, Suzanne Chen, and Yu-Hsuan Lin for helping design the survey, and thank Ankit Nehra, Mark Cwalinski, Randy Illum, and Hamzeh Zawawy for support throughout the project.

References

[1] Yeslam Al-Saggaf and Julie Maclean. 2024. Smartphone Privacy and Cyber Safety among Australian Adolescents: Gender Differences. *Information* 15, 10 (2024), 604.

[2] Android Developers. 2025. *Request location access at runtime.* https://developer.android.com/develop/sensors-and-location/location/permissions/runtime Android Developers Documentation.

[3] Android Developers. 2026. *Permissions on Android.* https://developer.android.com/guide/topics/permissions/overview Accessed: January 9, 2026.

[4] Android Developers. 2026. *Request runtime permissions.* https://developer.android.com/training/permissions/requesting#perm-groups Accessed: January 9, 2026.

[5] Android Open Source Project. 2025. *Android 12 and Android 12L release notes.* https://source.android.com/setup/start/android-12-release Android Open Source Project Documentation.

[6] Apple Inc. 2024. *About the privacy and security of Location Services in iOS, iPadOS, and watchOS.* https://support.apple.com/en-us/118390 Apple Support Documentation.

[7] Apple Inc. 2026. *Requesting Access to Protected Resources.* https://developer.apple.com/documentation/uikit/requesting-access-to-protected-resources Accessed: January 9, 2026.

[8] Apple Inc. 2026. *Requesting authorization to use location services.* https://developer.apple.com/documentation/corelocation/requesting-authorization-to-use-location-services Apple Developer Documentation.

[9] Apple Support. 2024. *About privacy and Location Services in iOS, iPadOS, and watchOS.* https://support.apple.com/en-us/102515 Accessed: January 10, 2026.

[10] Alex Berke, Geoffrey Ding, Christopher Chin, Karthik Gopalakrishnan, Kent Larson, Hamsa Balakrishnan, and Max Z Li. 2023. Drone delivery and the value of customer privacy: A discrete choice experiment with US consumers. *Transportation Research Part C: Emerging Technologies* 157 (2023), 104391.

[11] Bram Bonné, Sai Teja Peddinti, Igor Bilogrevic, and Nina Taft. 2017. Exploring decision making with Android's runtime permission dialogs using in-context surveys. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. 195–210.

[12] Joseph Cox. 2025. *Candy Crush, Tinder, MyFitnessPal: See the Thousands of Apps Hijacked to Spy on Your Location.* https://www.wired.com/story/gravy-location-data-app-leak-rtb/

[13] Joseph Cox. 2026. Inside ICE's Tool to Monitor Phones in Entire Neighborhoods. 404 Media. https://www.404media.co/inside-ices-tool-to-monitor-phones-in-entire-neighborhoods/ Accessed: January 9, 2026.

[14] Verena Distler, Matthias Fassl, Hana Habib, Katharina Krombholz, Gabriele Lenzini, Carine Lallemand, Lorrie Faith Cranor, and Vincent Koenig. 2021. A systematic literature review of empirical methods and risk representation

in usable privacy and security research. *ACM Transactions on Computer-Human Interaction (TOCHI)* 28, 6 (2021), 1–50.
[15] William Enck, Peter Gilbert, Seungyeop Han, Vasant Tendulkar, Byung-Gon Chun, Landon P Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol N Sheth. 2014. Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones. *ACM Transactions on Computer Systems (TOCS)* 32, 2 (2014), 1–29.
[16] Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, and David Wagner. 2011. Android permissions demystified. In *Proceedings of the 18th ACM conference on Computer and communications security*. 627–638.
[17] Adrienne Porter Felt, Serge Egelman, Matthew Finifter, Devdatta Akhawe, and David Wagner. 2012. How to ask for permission. *HotSec* (2012).
[18] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the eighth symposium on usable privacy and security*. 1–14.
[19] Huiqing Fu and Janne Lindqvist. 2014. General area or approximate location? How people understand location permissions. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society*. 117–120.
[20] Grand View Research. 2025. *Location Intelligence Market Size, Share, & Trends Analysis Report By Component (Software, Service), By Location Type (Indoor, Outdoor), By Deployment, By Application, By Vertical, By Region, And Segment Forecasts, 2025 - 2030.* Market Research Report GVR-2-68038-401-7. Grand View Research. https://www.grandviewresearch.com/industry-analysis/location-intelligence-market
[21] Darren Hayes, Christopher Snow, and Saleh Altuwayjiri. 2018. A dynamic and static analysis of the uber mobile application from a privacy perspective. *Journal of information systems applied research* 11, 1 (2018), 11.
[22] Sven Heitmann, Alexia Pagotto, and Christian Kray. 2025. Approximate vs. precise location in popular location-based services. *Journal of Location Based Services* 19, 1 (2025), 1–42.
[23] Jon M Jachimowicz, Shannon Duncan, Elke U Weber, and Eric J Johnson. 2019. When and why defaults influence decisions: a meta-analysis of default effects. *Behavioural Public Policy* 3, 2 (2019), 159–186. doi:10.1017/bpp.2018.43
[24] Hongbo Jiang, Jie Li, Ping Zhao, Fanzi Zeng, Zhu Xiao, and Arun Iyengar. 2021. Location privacy-preserving mechanisms in location-based services: A comprehensive survey. *ACM Computing Surveys (CSUR)* 54, 1 (2021), 1–36.
[25] Jon Keegan and Alfred Ng. 2021. *There's a Multibillion-Dollar Market for Your Phone's Location Data.* https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data
[26] Patrick Gage Kelley, Sunny Consolvo, Lorrie Faith Cranor, Jaeyeon Jung, Norman Sadeh, and David Wetherall. 2012. A conundrum of permissions: installing applications on an android smartphone. In *International conference on financial cryptography and data security*. Springer, 68–79.
[27] Rishabh Khandelwal, Asmit Nayak, Paul Chung, and Kassem Fawaz. 2024. Unpacking privacy labels: A measurement and developer perspective on google's data safety section. In *33rd USENIX Security Symposium (USENIX Security 24)*. 2831–2848.
[28] Brian Krebs. 2024. *The Global Surveillance Free-for-All in Mobile Ad Data.* https://krebsonsecurity.com/2024/10/the-global-surveillance-free-for-all-in-mobile-ad-data/
[29] Pedro Giovanni Leon, Blase Ur, Yang Wang, Manya Sleeper, Rebecca Balebako, Richard Shay, Lujo Bauer, Mihai Christodorescu, and Lorrie Faith Cranor. 2013. What matters to users? factors that affect users' willingness to share information with online advertisers. In *Proceedings of the ninth symposium on usable privacy and security*. 1–12.
[30] Kelly D Martin and Patrick E Murphy. 2017. The role of data privacy in marketing. *Journal of the Academy of Marketing Science* 45, 2 (2017), 135–155.
[31] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.
[32] Prolific. 2026. *Can I screen participants within my study?* https://researcher-help.prolific.com/en/articles/445165-can-i-screen-participants-within-my-study Accessed: January 9, 2026.
[33] Madelyn R Sanfilippo, Yan Shvartzshnaider, Irwin Reyes, Helen Nissenbaum, and Serge Egelman. 2020. Disaster privacy/privacy disaster. *Journal of the Association for Information Science and Technology* 71, 9 (2020), 1002–1014.
[34] Bingyu Shen, Lili Wei, Chengcheng Xiang, Yudong Wu, Mingyao Shen, Yuanyuan Zhou, and Xinxin Jin. 2021. Can systems explain permissions better? understanding users' misperceptions under smartphone runtime permission model. In *30th USENIX Security Symposium (USENIX Security 21)*. 751–768.
[35] Mohammad Tahaei, Ruba Abu-Salma, and Awais Rashid. 2023. Stuck in the permissions with you: Developer & end-user perspectives on app permissions & their privacy ramifications. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–24.
[36] Joshua Tan, Khanh Nguyen, Michael Theodorides, Heidi Negrón-Arroyo, Christopher Thompson, Serge Egelman, and David Wagner. 2014. The effect of developer-specified explanations for permission requests on smartphone user behavior. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 91–100.
[37] Richard H Thaler and Cass R Sunstein. 2009. *Nudge: Improving decisions about health, wealth, and happiness.* Penguin.
[38] Primal Wijesekera, Arjun Baokar, Ashkan Hosseini, Serge Egelman, David Wagner, and Konstantin Beznosov. 2015. Android permissions remystified: A field study on contextual integrity. In *24th USENIX Security Symposium (USENIX Security 15)*. 499–514.

A Survey

This is the full text copy of the Qualtrics survey. Italics indicate text not shown to participants. Lines indicate where questions are divided into separate pages. Upon entering the survey, participants are randomly assigned to 1 of 4 groups:

- *Control: Shown no request reasons (A)*
- *Exp group 1: Shown high quality reasons only (B)*
- *Exp group 2: Shown mix of high quality and low quality reasons (B and C)*
- *Exp group 3: Shown mix of high quality and ads related reasons (B and D)*

Your responses to this survey may be used in a research publication. All responses will be anonymized and any reports and presentations about the findings from this survey will not include any information that could identify you. By continuing in this survey, you acknowledge you are at least 18 years of age and consent to the use of your responses in research publications.

◯ Continue
◯ Exit

What is your Prolific ID?
(Text field; automatically filled from URL parameter.)

The following questions are redundant to recruitment criteria.

In which country do you currently reside?
(Drop down.)

What type of device do you use as your primary mobile phone?

◯ Android
◯ Apple/iOS
◯ I do not use a mobile phone

Participants who do not select the US and Android automatically exit survey.

What is your gender?

◯ Woman
◯ Man
◯ Non-binary

◯ Prefer to self-describe

What is your age in years?

◯ 18-24
◯ 25-34
◯ 35-44
◯ 45-54
◯ 55-64
◯ 65 or older

What is the highest level of education you have completed?

◯ Some high school or less
◯ High school diploma or GED
◯ Some college, but no degree
◯ Associates or technical degree
◯ Bachelor's degree
◯ Graduate or professional degree

How much do you agree with the following statement? This is an attention check. The correct answer is Agree.

◯ Strongly disagree
◯ Disagree
◯ Neutral
◯ Agree
◯ Strongly agree

Attention check; incorrect responses automatically exit survey.

For the following questions, please imagine you are using your real personal Android device.

Suppose you just downloaded a new Wallpaper app to use for the first time and you see the following dialog.
[Image from row 1 of Table 3, corresponding to participant experiment group is shown.]
Which button do you tap?

◯ Approximate
◯ Precise

Which button do you tap?

◯ While using the app
◯ Only this time
◯ Don't allow

Suppose you just downloaded a local news app to use for the first time and you see the following dialog.
[Image from row 2 of Table 3, corresponding to participant experiment group is shown.]
Which button do you tap?

◯ Approximate
◯ Precise

Which button do you tap?

◯ While using the app
◯ Only this time
◯ Don't allow

Suppose you just downloaded a new ride sharing app to use for the first time and you see the following dialog.
[Image from row 3 of Table 3, corresponding to participant experiment group is shown.]
Which button do you tap?

◯ Approximate
◯ Precise

Which button do you tap?

◯ While using the app
◯ Only this time
◯ Don't allow

What type of app did the previous screen ask about?

◯ A food delivery app
◯ A social media app
◯ A weather app
◯ A dating app
◯ A ride sharing app
◯ I don't know

What reason did the app provide for requesting access to your location?

◯ A. It did not provide a reason
◯ B. "To help get you to your destination, RideShare uses your location to find drivers nearby, improve pickups, support, and more."
◯ C. "Your location is needed for app functionality."
◯ D. "To help get you to your destination, RideShare uses your location to find drivers nearby, improve pickups, and support our advertising programs."
◯ E. "To seamlessly provide door to door service."
◯ F. I don't know

(A-D are real options, where the correct option depends on the experiment group.)

Please rate your level of agreement with the following statement.
"I have control over what information gets collected and shared on my Android device"

	1 (Strongly disagree)	2	3	4	5 (Strongly agree)
Agreement	◯	◯	◯	◯	◯

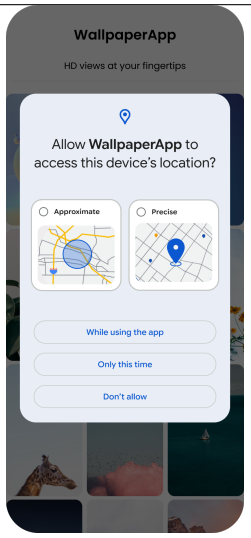
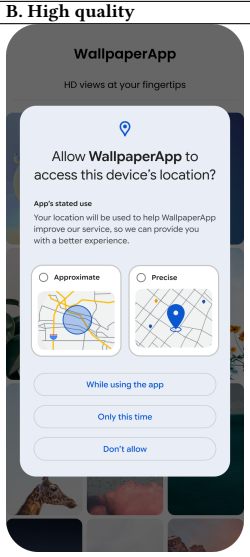
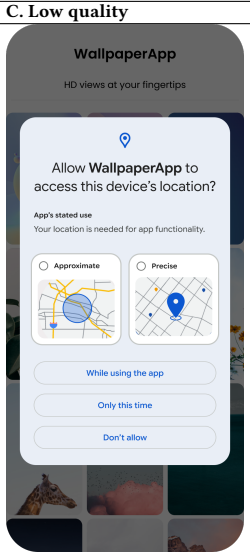
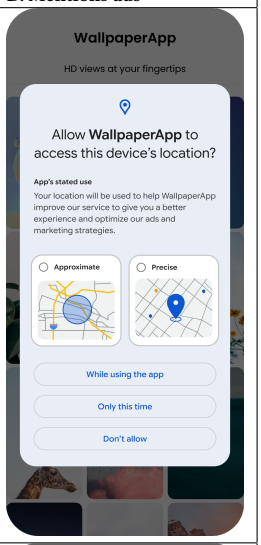
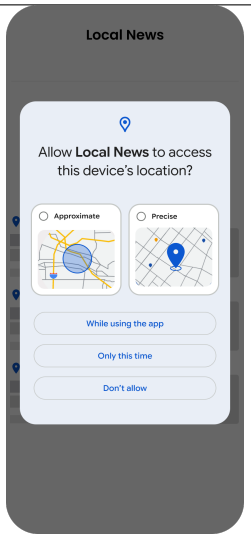
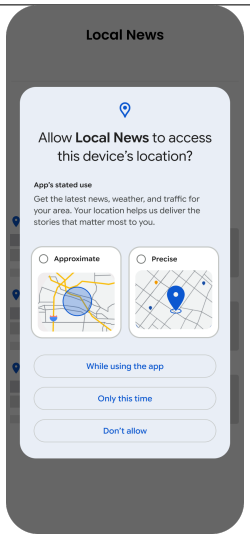
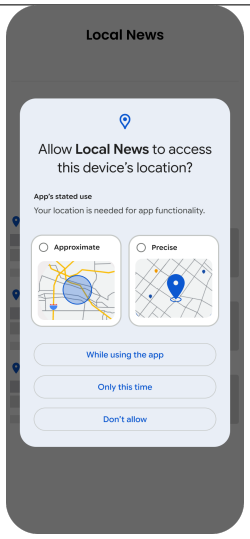
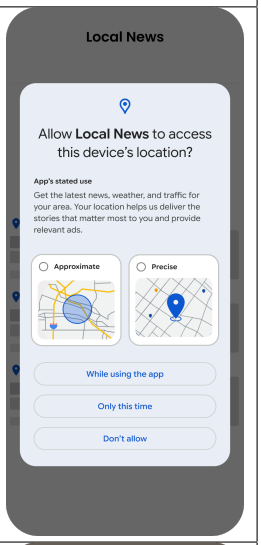
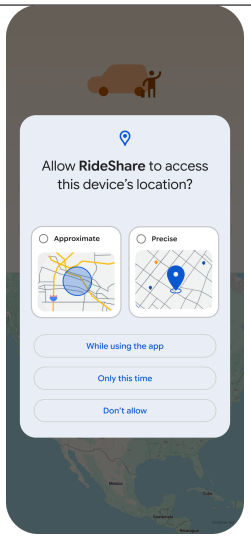
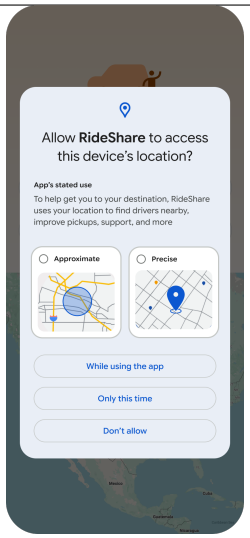
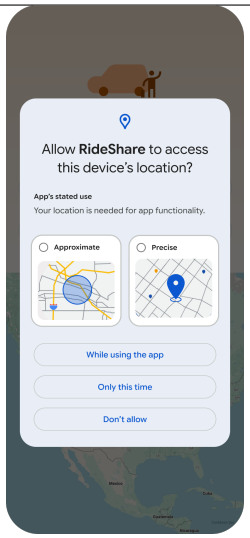
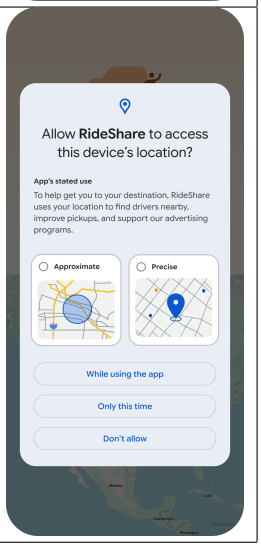
Thank you for your time! Do you have any additional comments? (Optional)

◯ No
◯ Yes, I would like to say: _____

B Android and iOS location request dialogs

Figure 4 provides examples of location permission dialogues from Android [2] and iOS [9].

Table 3: Request dialogs shown to participants for each app and reason tested, corresponding to Table 1.

#	App type	A. Control: None	B. High quality	C. Low quality	D. Mentions ads
1	Wallpaper				
2	Local news				
3	Ride share				

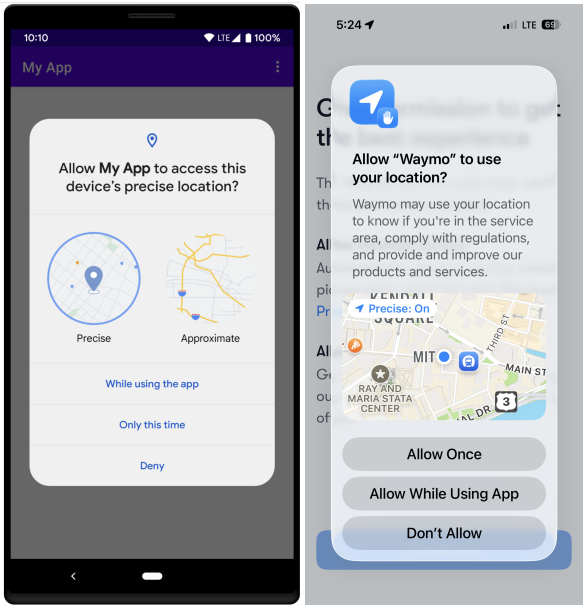


Figure 4: Examples of location permission dialogs from (left) Android and (right) iOS.

C Survey and participant details

Table 3 shows the request dialogues shown to participants for each app and reason tested, corresponding to Table 1.

Participants were recruited via the Prolific platform (https://www.prolific.com), using a US representative sample and paid $1.25 USD. We used Prolific's tools to recruit Android users. We advertised the survey as a study about "Android user choices" and the description said: "This study asks about your preferences when you install new Android apps. It also asks for your demographic information." It listed Android use and US residency as eligibility requirements.

We used additional screening questions at the start of our survey to confirm participants were both US residents and used Android as their primary mobile phone. Participants were automatically exited (screened out) from the survey if they did not pass the prescreening questions confirming that they were US residents and used Android as their primary mobile device. These screened out participants were paid $0.14 for their short time, as recommended by Prolific. After prescreening the sample includes 2,729 participants. We further filtered out 4 participants who failed the first attention check and 145 participants who failed the second attention check.

N=2,579 total participants were included in the analysis. Table 4 shows their responses to the demographic questions. Table 5 shows how they were evenly distributed across the four experiment groups.

D Analysis details

We evaluate participant choices corresponding to the request reason they were shown (A-D), corresponding to the experiment setup in Table 1. Note that participants in experiment

Table 4: Participant demographic details.

	n	%
Total	2579	100
Gender		
Woman	1285	49.7
Man	1250	48.4
Other (Nonbinary or self-describe)	44	1.7
Age in years		
18 - 24	290	11.2
25 - 34	507	19.6
35 - 44	484	18.7
45 - 54	413	16.0
55 - 64	582	22.5
65 or older	303	11.7
Education level		
Some high school or less	25	1.0
High school diploma or GED	385	14.9
Some college, but no degree	514	19.9
Associates or technical degree	381	14.7
Bachelor's degree	953	36.9
Graduate or professional degree	321	12.4

Table 5: Participant distribution across experiment groups.

Experiment group		n	%
0	Control: Shown no reasons	633	24.5
1	Shown high quality reasons (B)	674	26.1
2	Shown mix of high/low quality (B/C)	666	25.8
3	Shown mix of high quality/ads related (B/D)	606	23.5

groups 2 and 3 (see Table 5) had a 50% chance of seeing either reason B or C and D, respectively, resulting in a different number of responses for each request reason.

Aggregated results are shown in Tables 6 - 7. For the regression analysis, we transform the raw response data into an intermediary table with a row for each response to the app questions, i.e., 3 separate rows for each participant, corresponding to the 3 separate apps they responded for, with a column indicating the version of the request shown (A-D), which is included as an independent variable.

Table 6: Location access choices.

		Request reason shown			
Wallpaper app					
Choice	**Overall (n=2579)**	**A (633)**	**B (1314)**	**C (330)**	**D (302)**
Precise	19.1%	21.3%	17.9%	20.9%	17.9%
Approximate	38.0%	37.8%	38.3%	35.2%	40.1%
Don't allow	42.9%	40.9%	43.8%	43.9%	42.1%
Local news app					
Choice	**Overall (n=2579)**	**A (633)**	**B (1306)**	**C (338)**	**D (302)**
Precise	23.9%	24.8%	23.4%	24.6%	23.5%
Approximate	59.2%	59.7%	59.4%	55.9%	60.9%
Don't allow	16.9%	15.5%	17.2%	19.5%	15.6%
Ride share app					
Choice	**Overall (n=2579)**	**A (633)**	**B (1314)**	**C (333)**	**D (299)**
Precise	88.5%	88.5%	88.7%	88.6%	87.3%
Approximate	9.1%	9.5%	8.8%	8.7%	10.4%
Don't allow	2.4%	2.1%	2.5%	2.7%	2.3%

Table 7: Location access choices, restricted to participants who allowed location access.

		Request reason shown			
Wallpaper app					
Choice	**Overall (n=1472)**	**A (374)**	**B (738)**	**C (185)**	**D (175)**
Precise	33.5%	36.1%	31.8%	37.3%	30.9%
Approximate	66.5%	63.9%	68.2%	62.7%	69.1%
Local news app					
Choice	**Overall (n=2143)**	**A (535)**	**B (1081)**	**C (272)**	**D (255)**
Precise	28.7%	29.3%	28.2%	30.5%	27.8%
Approximate	71.3%	70.7%	71.8%	69.5%	72.2%
Ride share app					
Choice	**Overall (n=2517)**	**A (620)**	**B (1281)**	**C (324)**	**D (292)**
Precise	90.7%	90.3%	91.0%	91.0%	89.4%
Approximate	9.3%	9.7%	9.0%	9.0%	10.6%

Table 8: Logistic regression results testing which factors impact users' likelihood to allow (approximate or precise) versus deny the location access requests.

Predictor	**Log odds**	**Odds Ratio**	**95% CI**	**p-value**
Intercept	0.251^{*}	1.285	[1.053, 1.569]	0.013
Request reason (Ref: A; Control)				
B	-0.112	0.894	[0.737, 1.085]	0.257
C	-0.121	0.886	[0.677, 1.161]	0.381
D	-0.039	0.961	[0.727, 1.271]	0.782
App type (Ref: Wallpaper)				
LocalNews	1.336^{***}	3.806	[2.911, 4.975]	<0.001
RideShare	3.508^{***}	33.372	[18.835, 59.129]	<0.001
Interaction effects (Ref: A x Wallpaper)				
B x LocalNews	-0.012	0.988	[0.715, 1.365]	0.941
C x LocalNews	-0.141	0.869	[0.561, 1.347]	0.529
D x LocalNews	0.041	1.042	[0.651, 1.669]	0.864
B x RideShare	-0.085	0.918	[0.466, 1.807]	0.805
C x RideShare	-0.151	0.860	[0.349, 2.119]	0.743
D x RideShare	-0.094	0.911	[0.345, 2.403]	0.850
Gender (Ref: Male)				
Female	0.083	1.087	[0.961, 1.229]	0.184
Other	-0.511^{*}	0.600	[0.388, 0.928]	0.022
Age (Ref: 18 - 34)				
35 - 54	0.113	1.120	[0.966, 1.299]	0.135
55+	0.249^{**}	1.283	[1.103, 1.493]	0.001
Education (Ref: No Bachelors degree)				
Bach. degree	-0.143^{*}	0.867	[0.761, 0.988]	0.032
Grad. degree	0.06	1.062	[0.873, 1.293]	0.547
Observations = 7737 Pseudo R-squared = 0.1874				

Table 9: Logistic regression results testing which factors impact users' likelihood to allow precise (versus approximate) location access.

Predictor	Log odds	Odds Ratio	95% CI	p-value
Intercept	-0.685^{***}	0.504	[0.393, 0.646]	<0.001
Request reason (Ref: A; Control)				
B	-0.191	0.826	[0.636, 1.074]	0.154
C	0.045	1.046	[0.725, 1.508]	0.811
D	-0.234	0.792	[0.539, 1.163]	0.234
App type (Ref: Wallpaper)				
LocalNews	-0.301^{*}	0.740	[0.558, 0.981]	0.036
RideShare	2.821^{***}	16.796	[11.951, 23.606]	<0.001
Interaction effects (Ref: A x Wallpaper)				
B x LocalNews	0.138	1.148	[0.811, 1.626]	0.436
C x LocalNews	0.023	1.024	[0.630, 1.663]	0.925
D x LocalNews	0.174	1.190	[0.716, 1.977]	0.503
B x RideShare	0.276	1.318	[0.866, 2.007]	0.197
C x RideShare	0.049	1.050	[0.581, 1.898]	0.872
D x RideShare	0.137	1.147	[0.630, 2.085]	0.654
Gender (Ref: Male)				
Female	0.008	1.008	[0.888, 1.145]	0.897
Other	-0.11	0.895	[0.525, 1.528]	0.685
Age (Ref: 18 - 34)				
35 - 54	0.124	1.132	[0.966, 1.326]	0.125
55+	0.257^{**}	1.294	[1.103, 1.414]	0.001
Education (Ref: No Bachelors degree)				
Bach. degree	-0.089	0.914	[0.797, 1.049]	0.202
Grad. degree	-0.001	0.999	[0.821, 1.216]	0.993
Observations = 6132 Pseudo R-squared = 0.2894				

Table 10: Logistic regression robustness test results, testing whether the request reason had a significant effect on participants' choice to allow location access for the RideShare app, restricted to participants who correctly identified the request reason they saw for the RideShare app.

Predictor	Log odds	Odds Ratio	95% CI	p-value
Intercept	3.995^{***}	$5.430700e+01$	[19.347, 152.443]	<0.001
Request reason (Ref: A; Control)				
B	-0.878	$4.160000e-01$	[0.161, 1.069]	0.069
C	-0.508	$6.020000e-01$	[0.072, 5.062]	0.640
D	18.658	$1.267540e+08$	$[0.000, inf]$	0.999
Gender (Ref: Male)				
Female	-0.11	$8.960000e-01$	[0.357, 2.249]	0.815
Other	-1.105	$3.310000e-01$	[0.038, 2.858]	0.315
Age (Ref: 18 - 34)				
35 - 54	0.168	$1.183000e+00$	[0.419, 3.338]	0.751
55+	0.584	$1.792000e+00$	[0.572, 5.614]	0.317
Observations = 829 Pseudo R-squared = 0.0337				

Table 11: Logistic regression robustness test results, testing whether the request reason shown had a significant effect on participants' choice to allow precise versus approximate location access for the Ride Share app, restricted to participants who correctly identified the request reason they saw for the Ride Share app.

Predictor	Log odds	Odds Ratio	95% CI	p-value
Intercept	2.131^{***}	8.425	[4.978, 14.258]	<0.001
Reason shown (Ref: A; Control)				
B	-0.401	0.670	[0.423, 1.061]	0.088
C	0.176	1.193	[0.348, 4.088]	0.779
D	0.526	1.691	[0.218, 13.094]	0.615
Gender (Ref: Male)				
Female	-0.016	0.984	[0.622, 1.558]	0.946
Other	-0.89	0.411	[0.108, 1.566]	0.193
Age (Ref: 18 - 34)				
35 - 54	0.302	1.353	[0.783, 2.336]	0.278
55+	0.353	1.423	[0.823, 2.461]	0.206
Education (Ref: No Bachelors degree)				
Bach. degree	-0.233	0.792	[0.494, 1.271]	0.335
Grad. degree	0.403	1.496	[0.649, 3.452]	0.344
Observations = 809 Pseudo R-squared = 0.01887				