UX Implementation Guide

INCOGNIA™

How to Request Location Permissions from Mobile Users

Tips for Achieving High Opt-in Rates

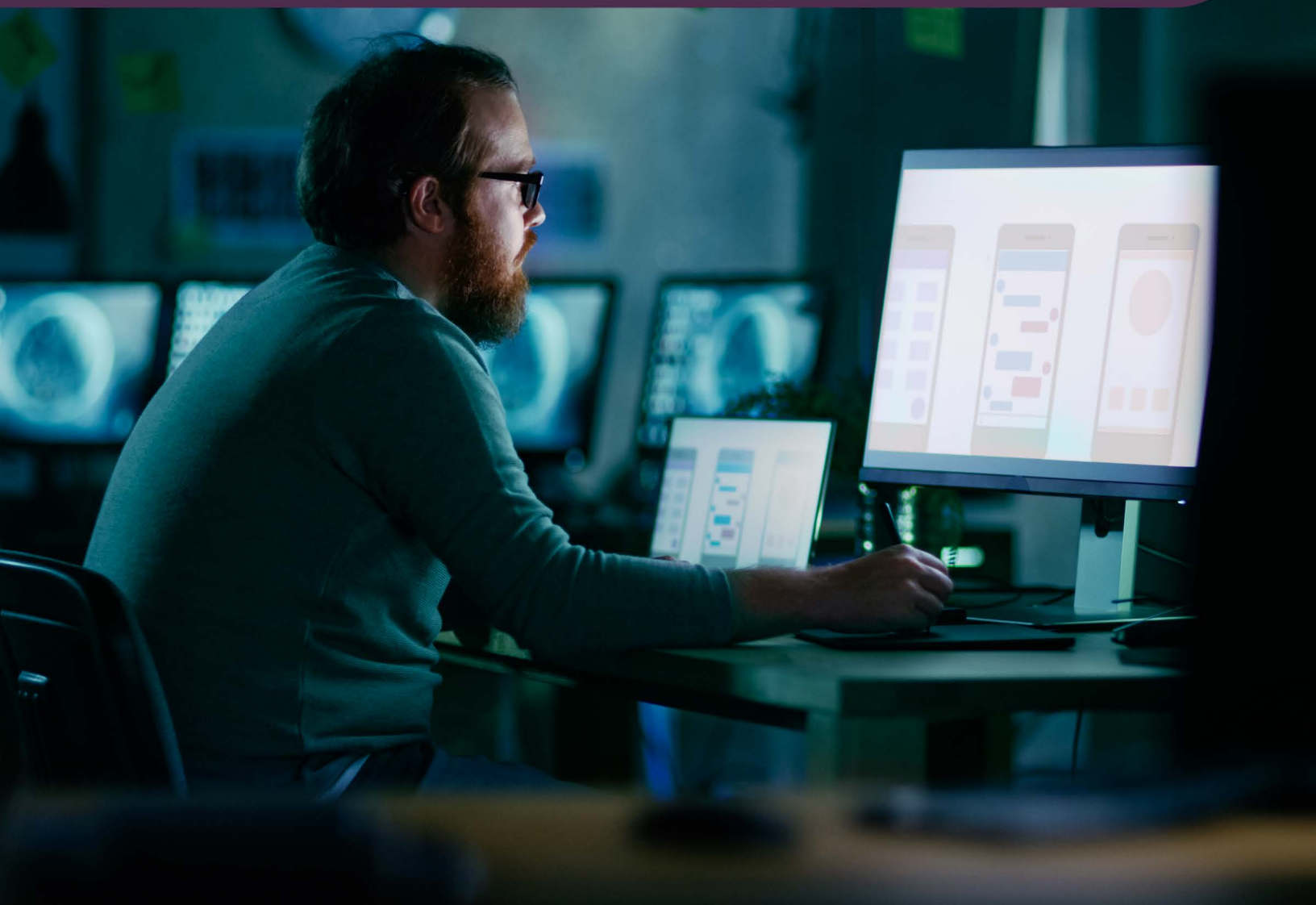


Table of Contents

01
Overview

This document describes how to optimize the request for location permission in mobile applications and achieve increased user opt-in rates. Companies following the best practices provided by Incognia have been able to achieve opt-in rates greater than 90%.

02
The impact of location opt-in requests on user conversion

Requesting location permission from the user impacts conversion just like any other moment in the mobile user experience. As with other critical points in the digital user journey, such as filling out a form or checking out of a shopping cart, conversion rates can vary considerably based on the context, language and design used to frame the request.

A comparison chart of the conversion rate of different types of online user interactions is shown below.

~21%
Online Forms

~5% - 74%
E-commerce Shopping Cart

Amazon prime has the highest conversion rate at **74%**

24% - 96%
Location Permissions Opt-In

Depending on the market segment and user messaging

Online Form Fill
Asking users to fill out forms can be frustrating and typically leads to a low conversion rate [1].

Shopping Cart
The e-commerce shopping cart conversion rate is very variable, ranging between 5% and 74%. Amazon Prime, which has achieved the best conversion rate in the e-commerce industry with its “single click” check-out, still fails to convert about 26% of the users that put items in their cart [2].

Location Permission
For location opt-In, Incognia has observed a wide range of acceptance rates, between 24% to 96% based on the design and timing of the messaging. Following best practices from Incognia, one company was able to increase opt-in rates for location permission from 45% to 93%

Key Takeaway

The design and timing of the location permission request message can significantly impact location opt-in rates

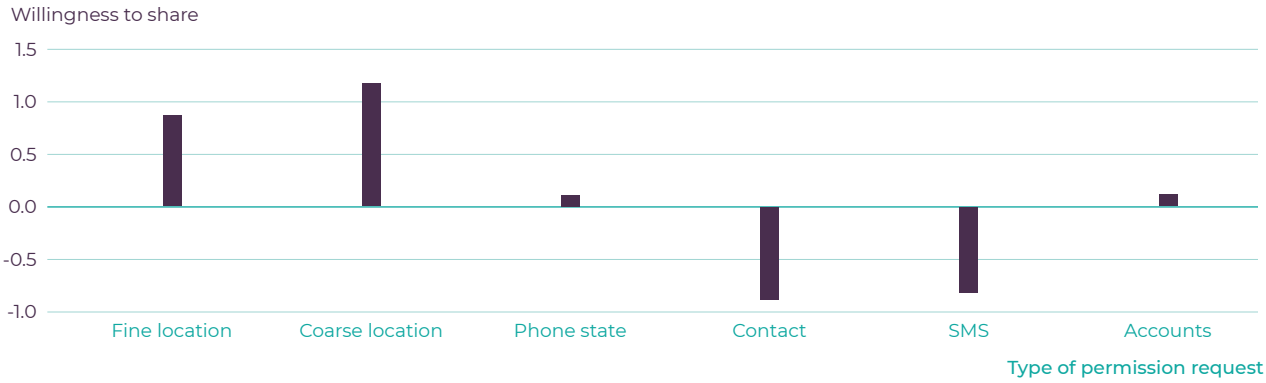
03

Willingness of users to share their location

There have been various academic UX research studies that assess the user's willingness to share their location with mobile apps. In a study by Carnegie Mellon University [3], they compare different types of permissions (location, phone state, contact, SMS and accounts) that users are asked to grant and the relative willingness by different types of users (conservative, advanced and fence-sitters) to share them. The result of this study, which comprised 800 apps and 1,200 people, was that location opt-in is the permission that is most easily shared by users in each of these groups

Comparison of willingness to share information

Positive value index: willing to share (max +2.0) | **Negative value index:** unwilling to share (min -2.0)



Key Takeaway

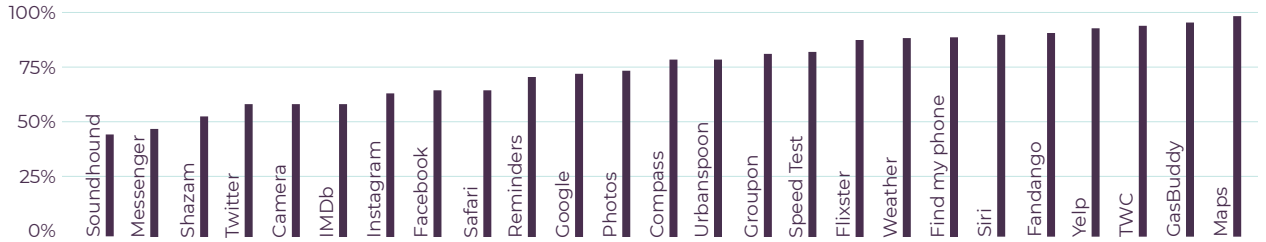
Users are more willing to share their location than share other types of sensitive mobile data.

04

Location permission opt-in rates

A study of the opt-in rate for location permission conducted at the University of California included a test of approximately 300 users using 700 apps. The apps that rely on location to add value to users (such as Google Maps, GasBuddy and Yelp) have opt-in rate of 90%, while for apps in which the rationale for requesting location is not rooted in a clear value exchange (such as audio streaming services like SoundHound and Shazam) the opt-in rate can dip as low as 50%.

Location Permission Opt-In % by Mobile App Type



If we consider the anonymized data collected from the 200M devices in Incognia's network, the location opt-in rates vary widely by industry.

Average and Highest User Location Opt-in Rate by Industry - Incognia Network Data

Online to Offline Delivery

The highest average percentage (~85%) is seen in the "Online to Offline" delivery apps. These apps ask users to share their exact location in exchange for convenience and a seamless delivery experience which is of clear value to the user..

Banking & Financial Services

The location opt-in rate is also very high for financial apps (averages 75% with peaks of over 95%). In this case, location is used as a signal to improve the security of financial transactions.

Ecommerce

The lowest average opt-in rate is seen in the eCommerce applications (~24%). The data suggests that users do not clearly understand the role played by location in their e-commerce experience and may be skeptical given the use of location-based advertisements by the eCommerce industry.

Another market vertical that has high location opt-in is **Mobile Gaming.** An average opt-in rate of 92% Is driven by the jurisdictional restrictions put in place to restrict the use of certain games to a specific geography.

Key Takeaway

When the user clearly understands why their location permission is being requested and can see the value they will receive in exchange, the user is more willing to share their location with the app.

05

Request location opt-in with a clear message

It is very important to explain clearly in the mobile app why the user is being asked to share their location. Mobile operating systems, such as iOS, offer developers the capability to add a Purpose String to the OS permissions request to explain the rationale behind the request. In the Purpose String, the developer can describe the additional functionality and user benefits enabled when location is shared.

A U.C. Berkeley study [5], investigated the effect of using the Purpose String on a pool of ~700 users. Using a test app the researchers added a randomized Purpose String to the permission request. The addition of a basic Purpose String, regardless of the specific message, increased the opt-in rate by 12%.

Opt-in With and Without a Purpose String

When exploring the differences among possible Purpose String message content, within a subset population

Request Type	% Allow
Permissions Request with a basic Purpose String	73.60%
Default OS Permissions Request (without Purpose String)	62.80%

of 59 users, the test showed that the most effective messaging can increase opt-in rate by 81%, as compared to the least effective message.

Opt-in with Different Types of Purpose Strings

Purpose String	% Opt-in
[Effective] A reason that clearly explains the users benefits	70.2%
[Basic] "This permission will allow the app to work properly"	52.5%
[Ineffective] An unclear message about Marketing and Advertising that could annoy the user	38.8%

However, based on the same study, the Purpose String seems to be an underutilized resource as only 19% of the permission requests analyzed included a developer-specified explanation.

Key Takeaway

Make use of the Purpose String on iOS to clarify the reason for requesting location permissions.

06

Categories and types of user messages

There are several explanations that may be added to a Purpose String and A/B tested to enable better user conversion. Example categories include:

	Message
User benefit This Purpose String describes how granting location permission will benefit the user's experience on the app.	*We use your location to manage your account and keep it safe*
User security This Purpose String describes how granting location permissions will keep the user's account secure.	*We use your location data to authenticate you and protect your account from fraud*
Information sharing This Purpose String promises or guarantees that the accessed information will not be misused, or that it will only be used for the described purpose.	*We'll only use your location information to improve your experience on this app. We do not sell or share your location data with third parties*
Data storage This Purpose String explains how and where the user's location data will be stored.	*Any location data you share with us will be securely encrypted and sent to our private servers*
Security This Purpose String describes how the accessed information will be protected against unauthorized access.	*We will encrypt your location data and store it securely on private servers.*

It's also possible to combine the different messages:

Security + Clear User Benefit

By sharing your location we can seamlessly authenticate you into your account without asking you for an OTP.	*We use your location to increase the security of your account and protect your in-app transactions against fraud.*	*This application uses your location to validate whether transactions made by your credit card are legitimate. This improves fraud prevention and keeps your account safe.*

Key Takeaway

Provide a clear and transparent explanation to encourage the user to provide location opt-in.

07

Strategies for requesting location permission

There are many different ways to structure the user location permissions request. Below are the best practices most frequently used by app developers today:

Three approaches to location permissions:

Minimalistic

Default OS Opt-in Request Only

Standard Operation System permission request alert. iOS allows adding a “purpose string”to explain more about the request for location permission.

Optimized

Primer Screen ⊕ OS Opt-in Request

Add a customized UX screen as pre-request to prime the user on the permission request prior to the standard OS permission alert.

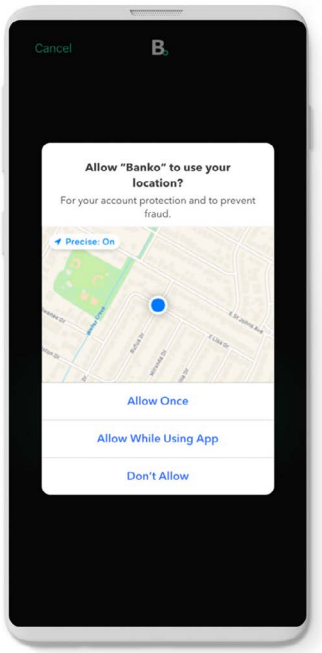
Reiterated

Two-step Looped Primer Screen ⊕ OS Opt-in Request

Present a customized UX screen to prime the user for the permission request. In case the user denies the permission request, add another screen to reiterate the request including the motivation before the user may definitely deny the permission request.

The Minimalist Approach: One chance to achieve opt-in

In this example, the developer only uses the Purpose String provided by the OS prompt to add context to the location opt-in request. This is both the simplest and most limiting way to ask for a location opt-in. The biggest drawback of only relying on the OS prompt to communicate the location request to the user is that it limits the amount of time you can request permissions. If the user denies the request, that remains their default until they manually change it in their device settings.



Optimized: Two screen request

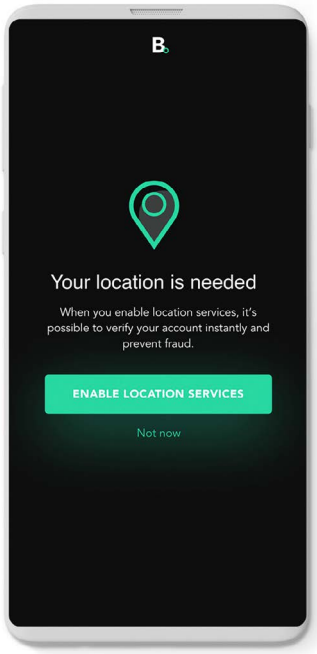
To increase the chances of catching users at the right time, apps often use a simple trick. They will show users a primer screen containing an unofficial request in advance of the OS prompt. This is called a “pre-permission” location screen and it gives app developers the opportunity to gauge the user’s likelihood of opting in to ensure the prompt is not wasted.

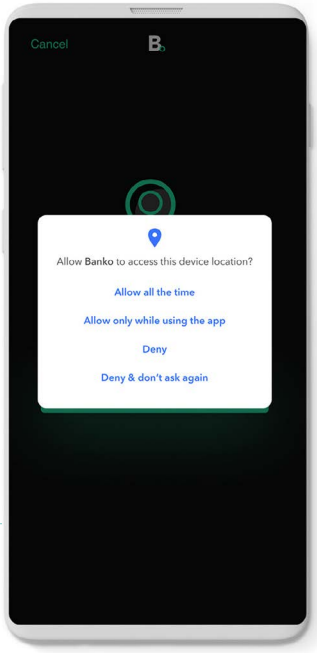
A pre-permission screen is an overlay containing completely customizable visuals and an expanded explanation of how granting location access will benefit app users and how their privacy will be protected . There’s no need to squeeze all the information into one sentence. Apps can make use of the screen space with custom text and visuals. Only once the user accepts the pre-permission request will the official dialog box be presented. If the user declines the primer, apps can decide to show permission requests again at another time.

There are two main benefits of this approach:

> The pre-permissions request screen can include some educational information and describe to users why it is important to accept the request and what benefits they receive in return.

> If users decide against accepting the permission, apps do not lose their chance to ask again. They can wait for a more appropriate time to ask again.

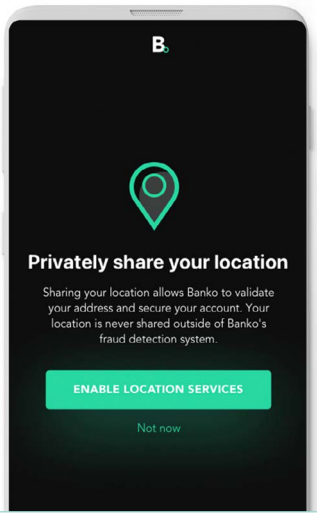


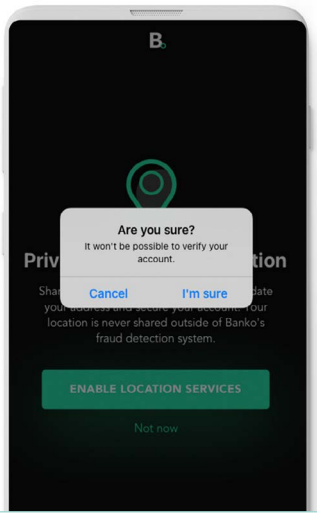


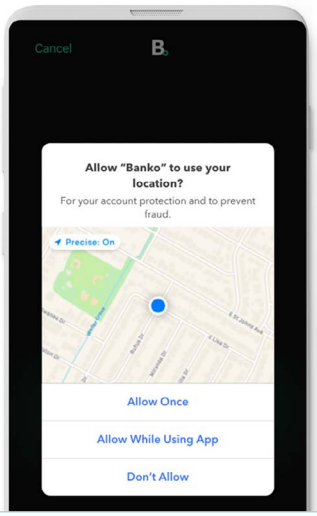
This is an example of a two screen request. It requires the user to approve the pre-permission or primer screen first and then respond to the official OS prompt.

Reiterated: Three screen request

With this approach, in the case where the user denies the unofficial pre-permissions screen, another screen can be immediately invoked to give the user another opportunity to accept.





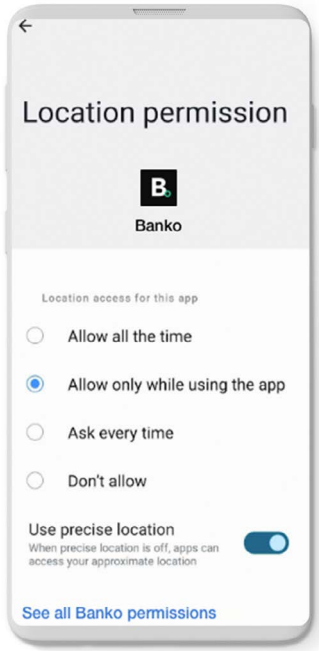


Clear Primers: Two primer screens with concise explanation of request + warning prompt if "no" is initially selected

Opt-In Request: Only prompt the user to opt-in with the OS dialog once they select "Yes" on the primer screen

The "reiterated" or three screen request, basically is a variation of the Optimal approach: In this case you show the first screen with an unofficial or "pre-permissions" request and if the user denies it, you can send the user immediately to another screen to give the user another opportunity to accept.

Recovery Plan: As much as you optimize your permission dialogue and user flow, it is inevitable that some users will make the decision to not share their data. But all is not lost! Even if the user has initially opted-out of the request, you can provide a new screen with additional context on the limitations of not opting in and a shortcut to the app "settings" so users can easily re-enable permissions. It's best practice to make it easy for users to change their location settings at any time.



Here is an example of the settings screen for location permission in your app

Key Takeaway

It is critical to provide a good explanation to the user about why location permission is being requested. The optimal results can be obtained by presenting a customized UX screen to prime the user before the official permission request. It is recommended to use either the "Optimal" or the "Reiterated" request approach.

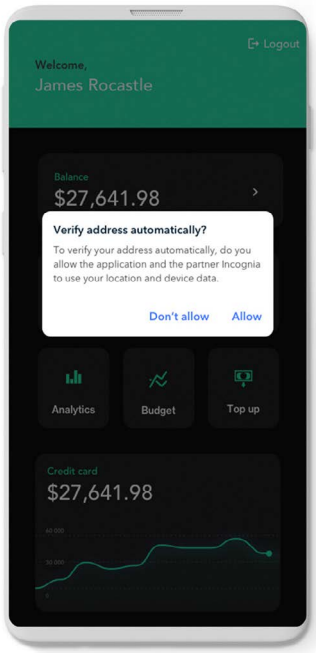
08
When to ask for location permission

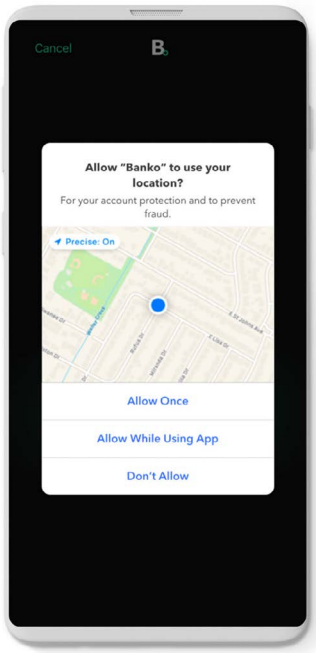
Users are more likely to agree to opt into location sharing when they are asked in the right context. The timing of the request should support the rationale provided in the prompt message. For example, when a user is searching for restaurants the app could request location to proactively suggest restaurants close by. Whenever possible, initiate a permission request when the user selects a feature that requires that permission. This approach gives the request important context and the user a feeling of control This makes it more likely for users to understand why the app is requesting it and leads to a higher conversion rate.

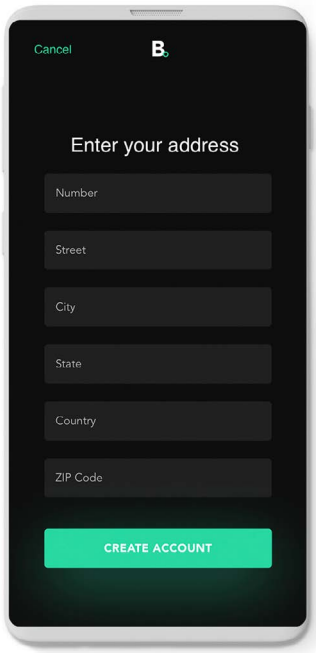
Example: Onboarding use case

Incognia provides real-time global mobile address validation during onboarding as part of identity verification. When a user provides their address to the mobile app, Incognia compares it with the user's current and historical location data to provide a risk assessment. To optimize the solution, the user should first be requested to share location before asking for the user address and passing to Incognia to make a risk assessment. Here is an example:

An example of this UX flow can be seen below: requesting location permission during onboarding

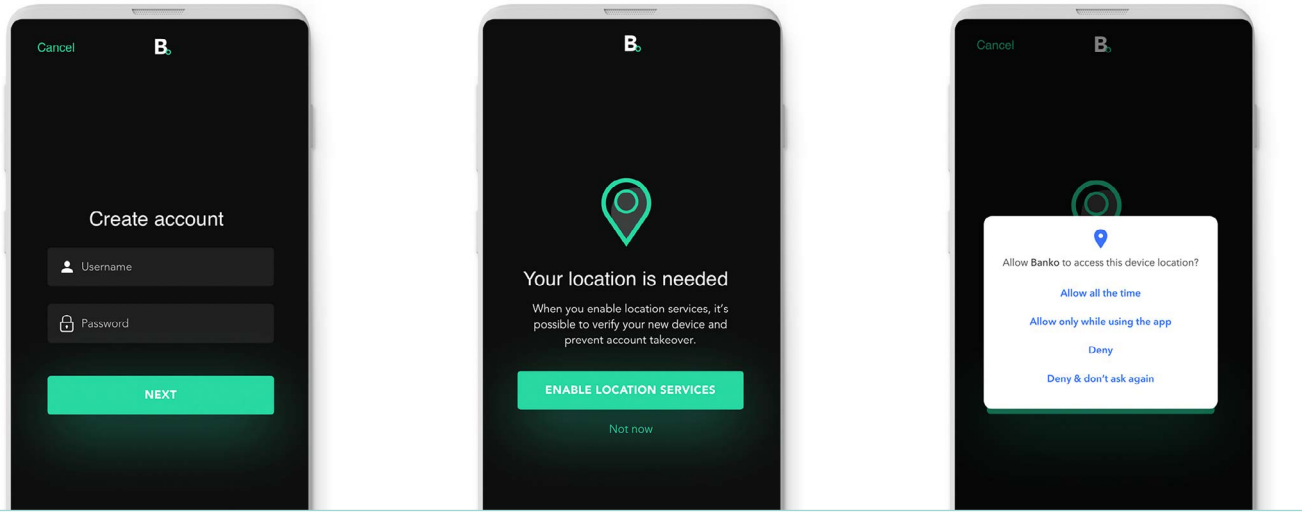






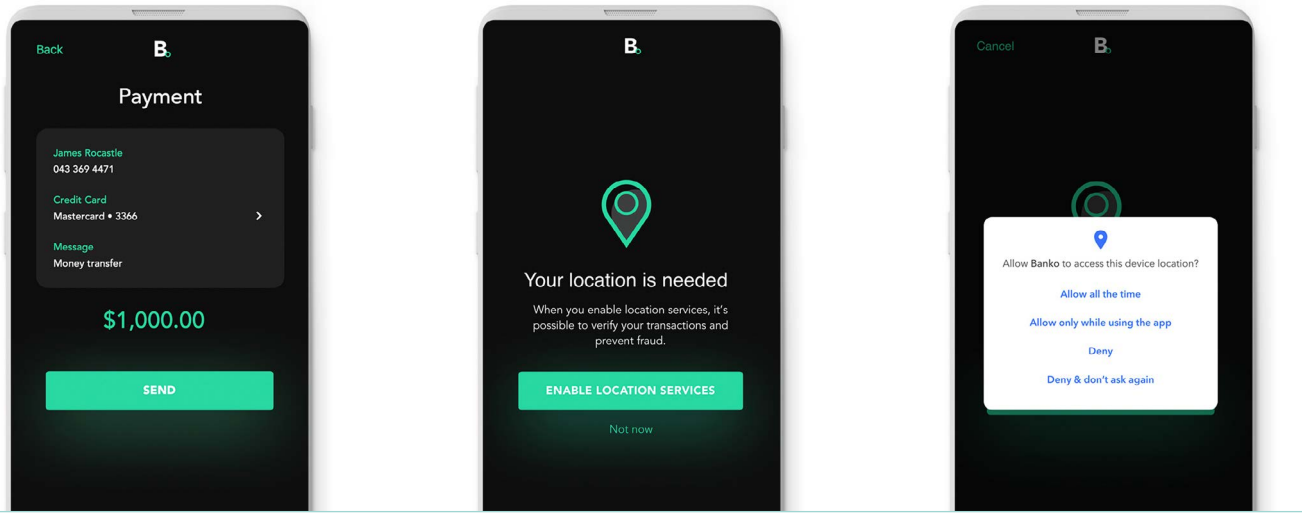
Example: Login use case

Incognia provides frictionless zero-factor authentication that helps protect mobile accounts from account takeover fraud at login. To secure each login, Incognia will need to gather a location event when a user is logging in and therefore will require the user to opt-in to location “while using” the app. The need for the permissions level “while using” could be messaged in a primer screen as outlined above. For example, the user could be asked for location permission when the user logs into their account for the first time or when they are asked to choose a new password or pin.



Sensitive transactions use case

Incognia helps secure customer mobile accounts during sensitive transactions, such as large transfers, account recovery or other risky in-app transactions. In this case, the user should be prompted to share their location before they are permitted to complete the transaction.



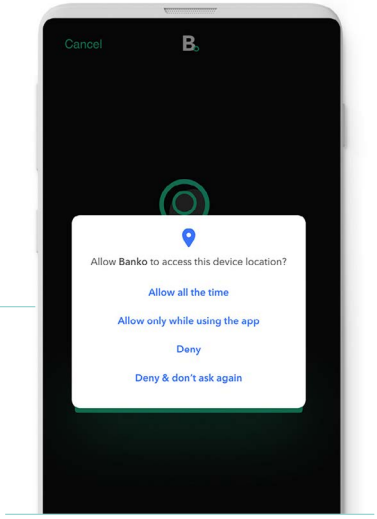
Key Takeaway

Being strategic about when to prompt the user with the location request will increase opt-in rates.

09
Case Study: Location opt-in rate increased from 45% to 93%

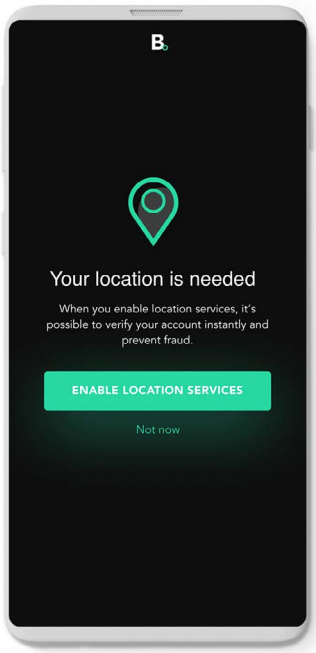
In working with a fintech and following the recommendations in this UX guide, Incognia was able to help improve the location opt-in rate for a fintech app from 45% to 93%. [6]

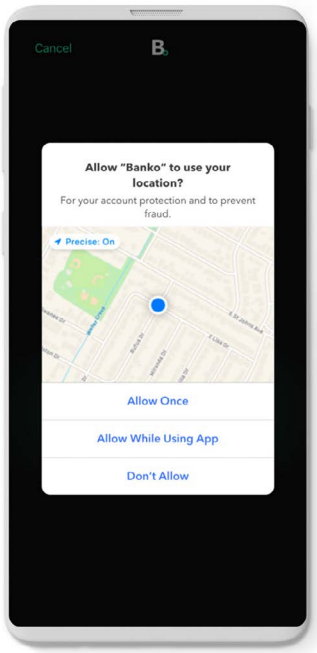
Prior to optimization, the fintech app was obtaining a 45% location opt-in rate from users. **The app was collecting permission from its users by prompting them with the a default OS message:**



The fintech did not optimize the moment they were asking for the permission and was not using any "purpose string" or any "pre-permissions" screen.

After consulting with Incognia and including the Incognia SDK for fraud prevention at sensitive transactions, the fintech chose to optimize by adopting the two screens their location permission request flow described above. The fintech:





01
Moved the permission request so users were prompted right before the risky transaction

02
Applied a pre-permissions screen to determine willingness to opt-in

03
Added an appropriate Purpose String to explain why permissions were needed

The opt-in rate increased from 45% to 93%.
Read the full location permissions case study details

Read the case ⟶

Key Takeaway

Being strategic about when to prompt the user with the location request will increase opt-in rates.

10

Declaring permissions requests to the app distribution stores

For optimal results using the Incognia SDK, the developer should request for a “precise location” in the App manifest (for example ACCESS_FINE_LOCATION permission in Android)

Read more ⟶

Before releasing an app with the Incognia SDK and the corresponding location permission requests, it is important to go through the new app release flow which is required by the app distribution stores, such as the Google Play Store and the App Store.

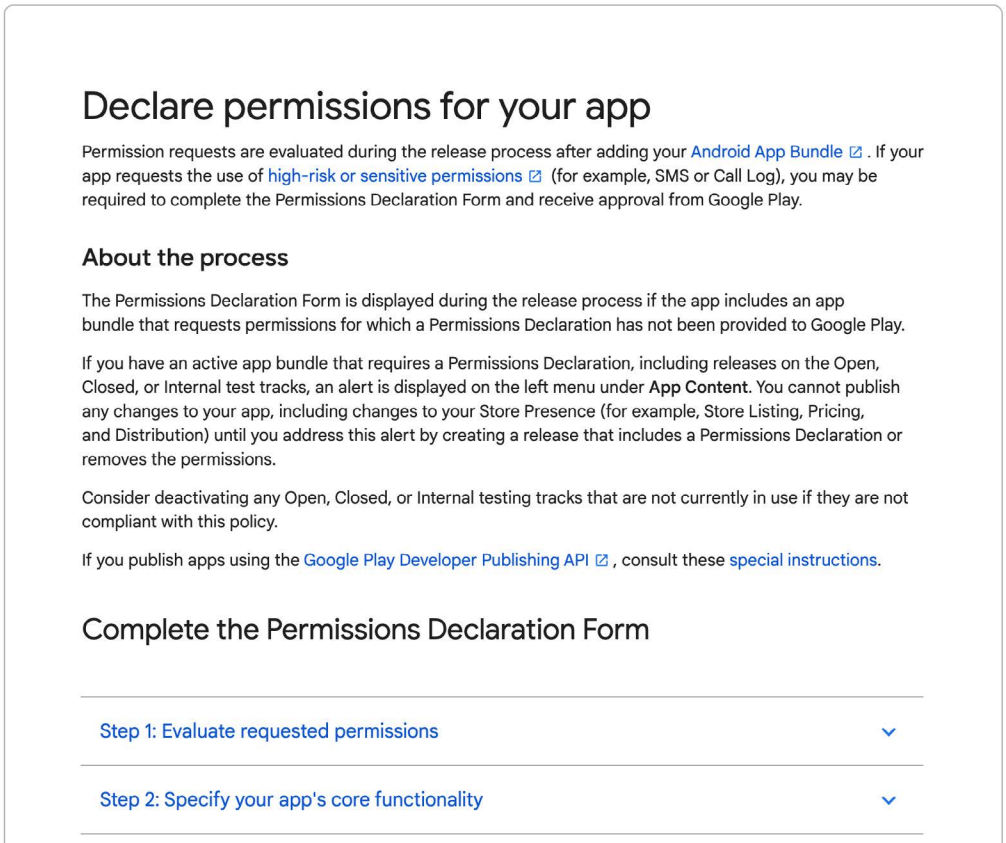
Google Play and Apple App stores require apps to substantiate their request for user location through an authorization process before launching the app in the market. In the app release flow, all permissions requested need to be declared to the distributing store. The Permissions Declaration Form is usually displayed during the App upload & release process. See below for an example of the permission declaration process that app developers need to follow with the leading app distribution stores:

See the example ⟶

See the example ⟶

Key Takeaway

Remember to declare that you are requesting location permissions from the user to the app store during the app release flow (Google Play and Apple App Store)



11
Conclusion

By implementing the recommendations and best practices in this UX guide, Incognia customers have successfully increased their location permission opt-in rate above 90%. Please do not hesitate to contact us if you have any questions.

12
Key Takeaways

In summary make sure your location permission strategy touches on these 4 points:

01
Be transparent
It is important that the user knows what data is being collected, how it will be used and what value they will derive in exchange.

02
Communicate the end-user value
Clearly communicate the advantages that the user will gain in exchange for sharing their location.

03
Time the request appropriately
Users are more likely to agree to permission requests when they get asked in the right context, for example before the feature that needs the permission is used.

04
Start with a primer or pre-permissions screen
Using a primer or pre-permissions screen is recommended to provide more context to the user and test out their willingness to opt-in before prompting them with the OS request.

13
References

[1] 101 Unbelievable Online Form Statistics & Facts for 2022

[2] Amazon FBA Conversion Rate

[3] Modeling Users' Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings (Jialiu Lin et al.)

[4] Location Privacy: User Behavior in the Field (Drew Fisher et al.)

[5] The Effect of Developer-Specified Explanations for Permission Requests on Smartphone User Behavior (Joshua Tan et al.)

[6] Incognia Location Permission Case Study

[7] How-to-series, Location Permission, 5 important considerations (Incognia ebook)

About Incognia

Incognia is a privacy-first location identity company that provides frictionless mobile authentication to banks, fintech and mCommerce companies, for increased mobile revenue and lower fraud losses. Incognia's award-winning technology uses location signals and motion sensors to silently recognize trusted users based on their unique behavior patterns and is a key enabler for Zero-Factor Authentication. Deployed in over 200 million devices, Incognia delivers a highly precise risk signal with extremely low false positive rates.