How-to Series

Location Permissions

5 Important Considerations

INCOGNIA™

Overview

The use of location data for mobile fraud prevention offers the opportunity to provide frictionless security for users. This guide provides a review of important topics related to managing user permission to collect location data. Included in this guide is information on how Incognia protects and manages the location data we collect, a review of the location features available on iOS and Android mobile devices and best practices for requesting permission to collect location data for fraud prevention.

Introduction

Today, around the globe, people consider their smartphones as a go to device. In the US, on average, US adults spend 4 hours and 16 minutes per day on their mobile devices[1], and it is often the first thing they reach for in the morning, and the last thing before going to bed. Even when not actively using their mobile devices people keep their devices close by, within reach. It is this close attachment between people and their mobile devices combined with the location technologies on the smartphone that enables the use of location behavior for fraud prevention. Incognia uses network signals and device intelligence to create a location fingerprint for each user, based on their unique location behavior that delivers a strong trust signal for mobile apps.

The use of Incognia for fraud prevention in mobile apps relies on network signals in order to build a user's unique location-based identity. This requires that location services are turned on, the mobile device is connected to a network: Wifi, Cellular, and that the user has given their permission to collect location data. With these features enabled Incognia can start detecting location points.

> The following sections describe important topics related to location data privacy, how data is collected from location technologies used on a mobile device and how to request location permissions for optimum performance.

[1] eMarketer, US Time Spent with Mobile 2021 (June 2021)

01

Location permission on mobile devices

iOS and Android mobile devices provide a number of user controls for setting permission related to the use of network signals, motion sensors, and the collection of location information. Understanding how these controls relate to the functioning of Incognia and how best to request user permissions will enable you to optimize the performance of Incognia within your mobile app.

Incognia technology is most effective when as many users as possible allow the use of location. Incognia relies on data from network signals in order to build a user's unique location-based identity. We see that user acceptance of use of location is high - 80% or higher - when the messaging is clear on the use and benefit to the user. Therefore, it is important to request permission to use location at a moment that most users will experience, such as when creating an account or when accessing a resource that depends on the location. If the permission request is too hidden, or linked to an infrequently used feature in the app, fewer users will view the request and the acceptance rate will be lower. It is good practice, give the user the option to choose between saving the chosen option or being asked again every time this permission is required.

> Users that do not accept the location permissions, and do not have location technologies turned on, will not generate location data, thus, are not able to receive benefits from Incognia features.

02

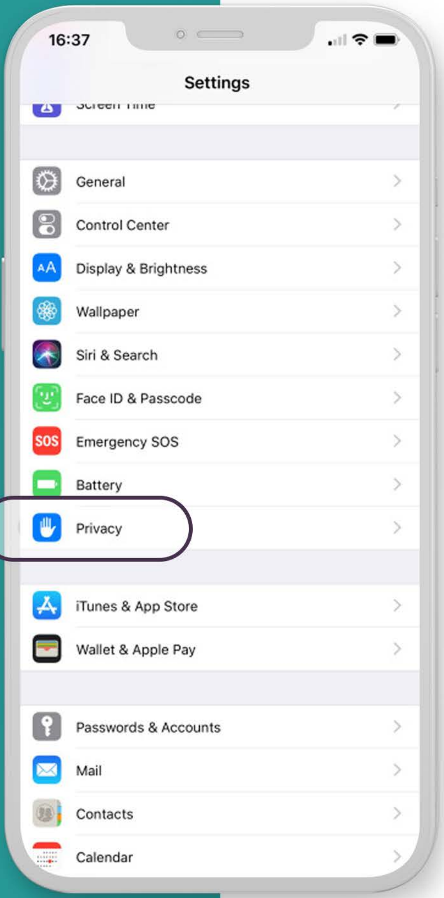
Types of location permission on iOS and Android devices

iOS - Location permissions

The iOS system includes several important features that relate to location permissions

User Control of Location Sharing

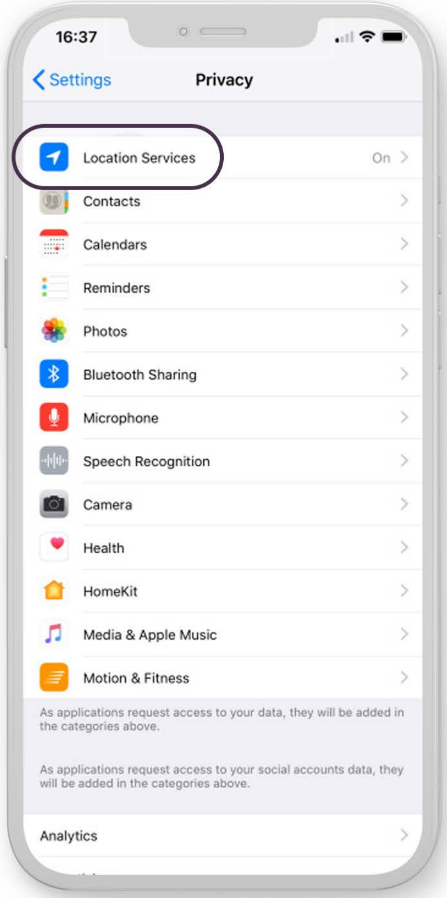
For iOS devices using iOS 14 or later, Apple users may choose between four options when deciding to share their location data with an app. However, before users decide to share their location with an app, it is required for the user to enable Location Services. This feature allows Apple and third-party apps and websites to use user location data to offer different location-based services.



16:37

Settings

- Screen Time
- General
- Control Center
- Display & Brightness
- Wallpaper
- Siri & Search
- Face ID & Passcode
- Emergency SOS
- Battery
- Privacy
- iTunes & App Store
- Wallet & Apple Pay
- Passwords & Accounts
- Mail
- Contacts
- Calendar



16:37

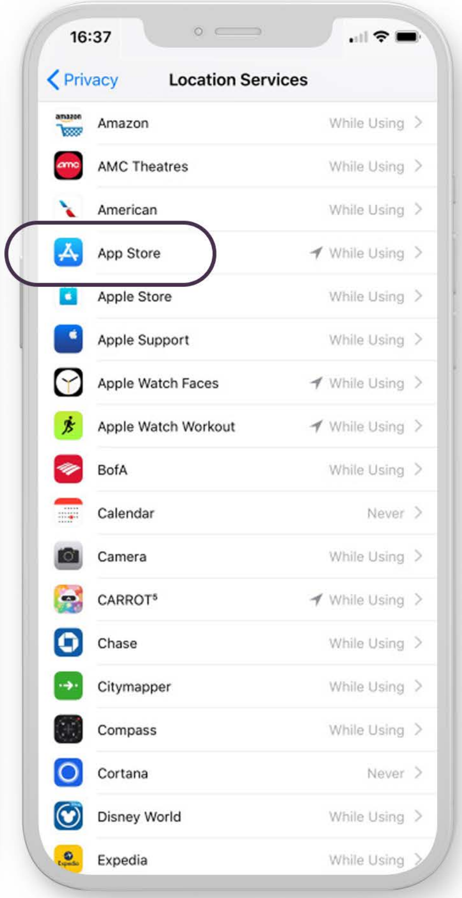
Settings — Privacy

Location Services	On
Contacts	
Calendars	
Reminders	
Photos	
Bluetooth Sharing	
Microphone	
Speech Recognition	
Camera	
Health	
HomeKit	
Media & Apple Music	
Motion & Fitness	

As applications request access to your data, they will be added in the categories above.

As applications request access to your social accounts data, they will be added in the categories above.

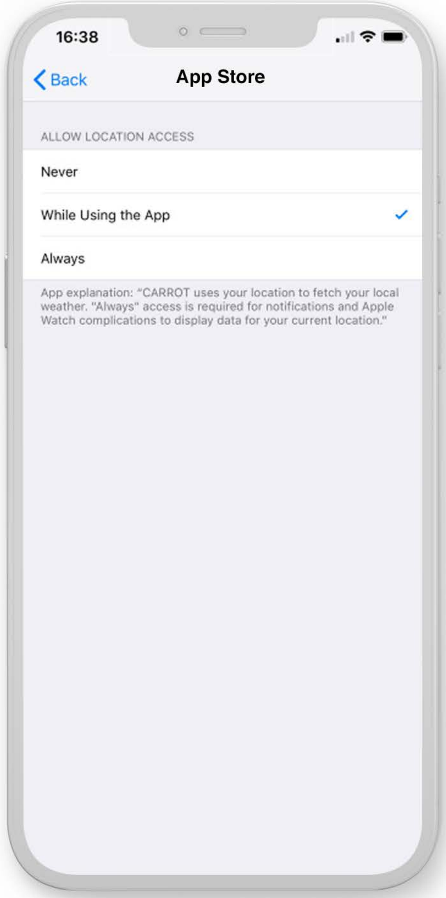
- Analytics



16:37

Privacy — Location Services

Amazon	While Using
AMC Theatres	While Using
American	While Using
App Store	While Using
Apple Store	While Using
Apple Support	While Using
Apple Watch Faces	While Using
Apple Watch Workout	While Using
BofA	While Using
Calendar	Never
Camera	While Using
CARROT⁵	While Using
Chase	While Using
Citymapper	While Using
Compass	While Using
Cortana	Never
Disney World	While Using
Expedia	While Using



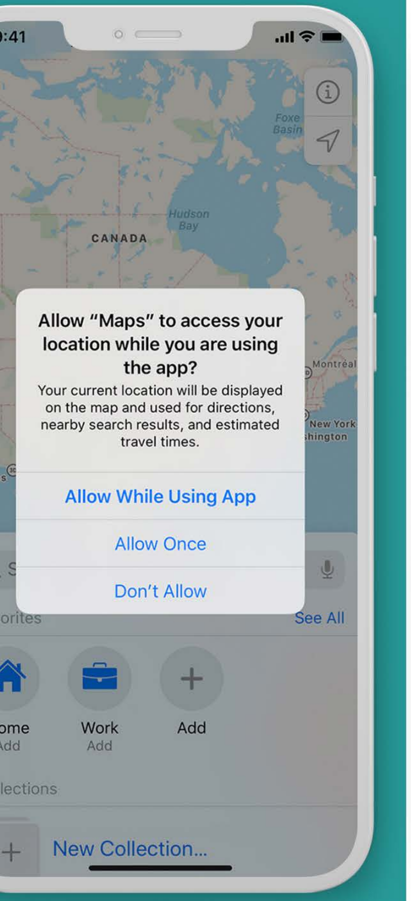
16:38

Back — App Store

ALLOW LOCATION ACCESS

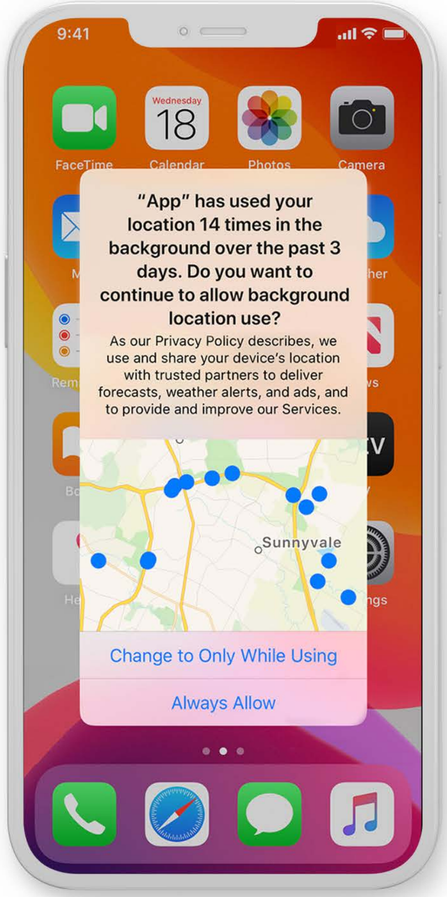
- Never
- While Using the App ✓
- Always

App explanation: "CARROT uses your location to fetch your local weather. "Always" access is required for notifications and Apple Watch complications to display data for your current location."



Allow “Maps” to access your location while you are using the app?

Your current location will be displayed on the map and used for directions, nearby search results, and estimated travel times.



“App” has used your location 14 times in the background over the past 3 days. Do you want to continue to allow background location use?

As our Privacy Policy describes, we use and share your device’s location with trusted partners to deliver forecasts, weather alerts, and ads, and to provide and improve our Services.

Be aware that by enabling location services, the user will allow different features related to location to be enabled, such as routing and traffic or location-based alerts. And to use those services, it is necessary that the user provides location permissions to each app, before it starts using user location data, choosing between the following:

Don’t allow

Prevents access to Location Services information.

Allow while Using the App

Allows access to Location Services only when the app or one of its features is visible on screen. If an app is set to While Using the App, the user might see the status bar turn blue with a message that an app is actively using location.

Allow Once

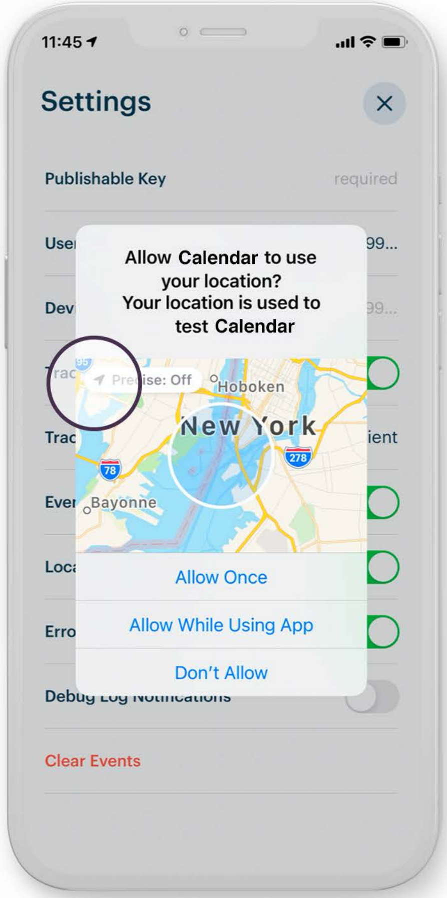
This allows the app to access the user’s location during that one interaction.

Always

This option allows access to location even when the app is in the background. It is only shown after the user selects “allows while using the app”. If the user has given this type of permission for previous versions of the OS, the new version will provide a new pop-up, so the user can confirm if “always” will continue to be the chosen option.

Precise and approximate location

A user can choose between providing an app precise location or an approximate location. According to Apple, precise location is “information that describes the location of a user or device with the same or greater resolution as a latitude and longitude with three or more decimal places”, while approximate location is “Information that describes the location of a user or device with lower resolution than a latitude and longitude with three or more decimal places, such as Approximate Location Services”. For Incognia, the use of precise location will provide a higher accuracy in location detection.

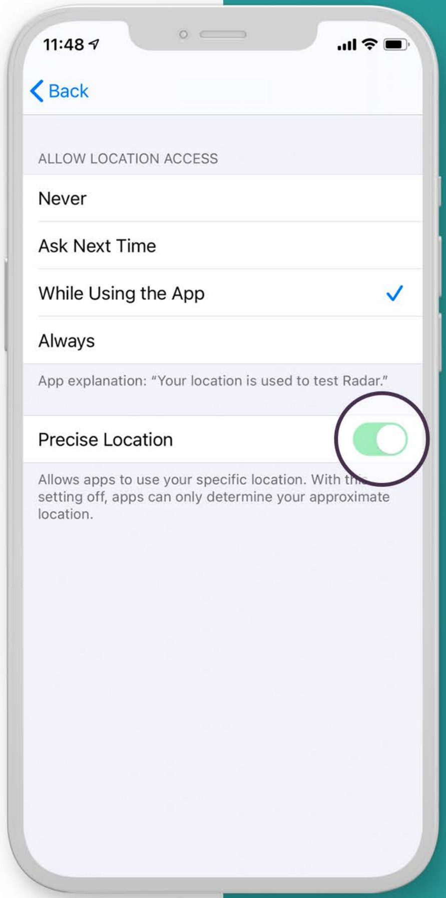


11:45

Settings

Publishable Key required

Allow Calendar to use your location?
Your location is used to test Calendar



11:48

Back

ALLOW LOCATION ACCESS

- Never
- Ask Next Time
- While Using the App ✓
- Always

App explanation: “Your location is used to test Radar.”

Precise Location

Allows apps to use your specific location. With the setting off, apps can only determine your approximate location.

App tracking transparency

Beginning with iOS 14, Apple introduced the AppTrackingTransparency framework to manage the app-tracking authorization request and status for any app that collects data about end users and shares it with other companies.

So, if your app shares data with Incognia, it is recommended to request the user's authorization using the AppTrackingTransparency framework available on iOS 14.

Use case	Messaging
Preventing new account fraud and account takeover	Share your location data with partner Incognia for protection against mobile fraud and account takeover on this application
Enabling frictionless secure onboarding	Share your location data with partner Incognia for frictionless secure onboarding on this application
Providing analysis on the user's physical behavior based on the device's behavioral data	Share your location data with partner Incognia for providing us with user physical behavior analysis

The iOS 15, yet to be released, will deliver a new privacy dashboard. In this dashboard, the user can check which apps are accessing their location - after the user gives their location permission - and how often it occurs.

Optimizing Incognia on iOS devices

For iOS apps, The Incognia SDK makes use of Apple's Visits Location Service, which requires the Always authorization. Not being able to acquire this authorization may greatly reduce the frequency of location-based features. The Incognia SDK checks the status of these permissions and changes its behavior accordingly.

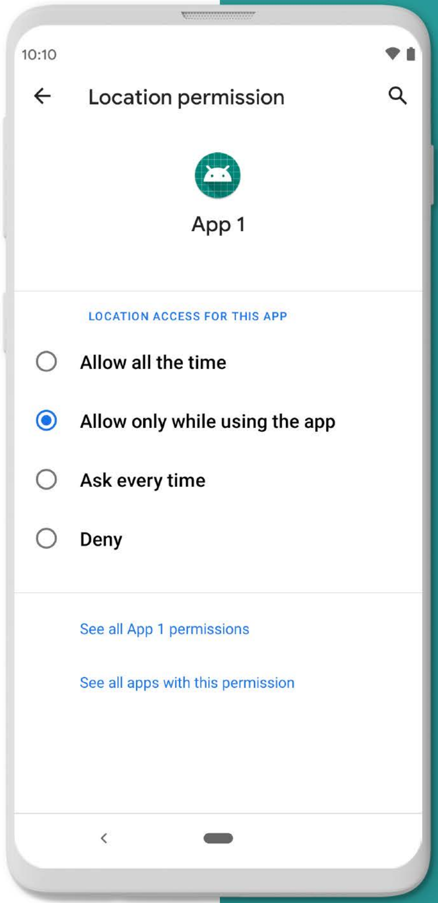
Android - Location permissions

The Android system has two different types of location permission: foreground and background location permission.

Foreground location

If an app has a feature that shares or receives location information only once, or for a defined amount of time, then that feature requires foreground location access, which means that location permission is given while the user is using the app, or only that defined time or even the option of denial. And, the newest Android version, yet to be released, will also have the possibility to choose between fine or coarse location, as currently supported in ioS.

According to Android developers, removing location or changing it from background to foreground can help apps be battery-efficient and avoid poor app ratings when users don't want to share their location. So, apps are always challenged to prove why they need user location. When it comes to Incognia, our technology was built based on optimizing not only the user experience but also battery consumption. The Incognia SDK consumes just 0.5% of a device's battery in 24 hours. So, we encourage users to allow background location to extract maximum value from using Incognia to protect their mobile journey against fraud, without adding friction.


10:10

Location permission

App 1

LOCATION ACCESS FOR THIS APP

○ Allow all the time

● Allow only while using the app

○ Ask every time

○ Deny

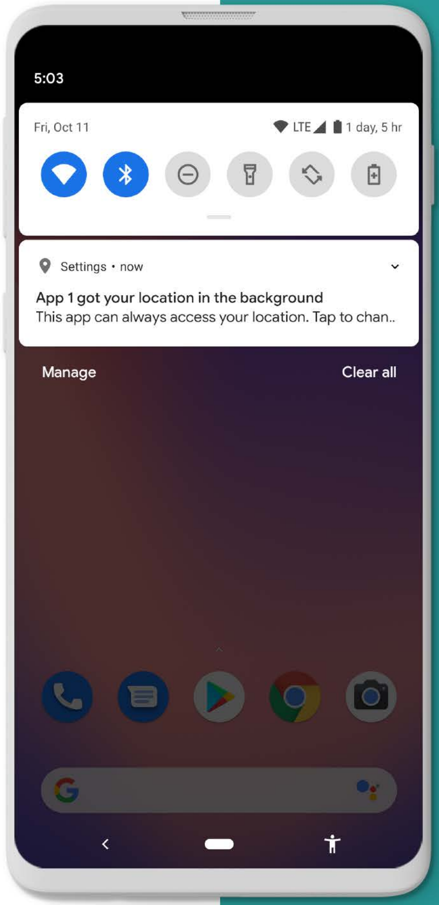
See all App 1 permissions

See all apps with this permission

Background permission

Asking for background location permission can apply to apps that have a feature that constantly shares location in different situations, such as sharing with other users or when Geofencing is on. On Android 11, users must enable background location on a settings page, as shown.

Android has a background access location reminder, which makes the user aware of the apps accessing their location and makes it easier for the user to decide if they want to keep those permissions on or maybe turn them off.



5:03

Fri, Oct 11

LTE 1 day, 5 hr

Settings • now

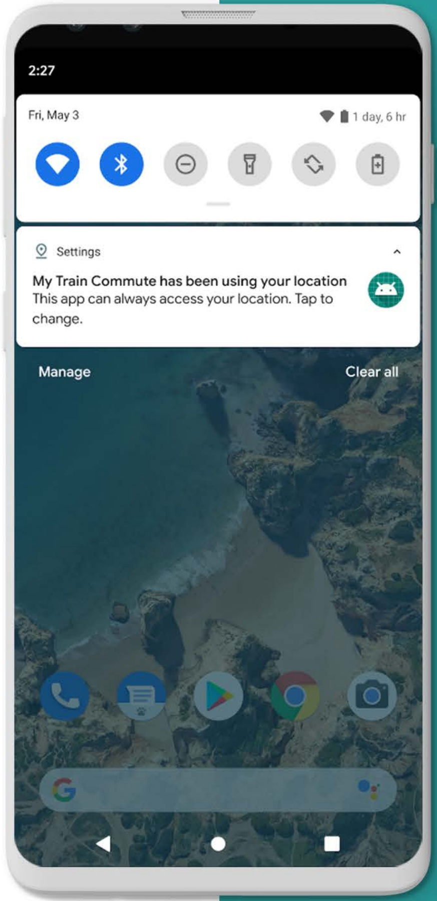
App 1 got your location in the background

This app can always access your location. Tap to chan..

Android provides an example of clear messaging that shows the benefits of accepting the location permissions. Due to its size, this messaging could be added to privacy policies as the complete version and or reduced to fit to the location permission request:

> **This app needs [Background] Location permission**
>
> “This app collects location data to enable security and fraud prevention features, such as address verification and transaction validation[, even when the app is closed or not in use]. In order to be able to do that, the app and our partner Incognia need to have access to your [background] location. Incognia will collect GPS, Wifi, Telephony [and Bluetooth] data and use it to provide context to your current location, protecting your transactions by preventing fraud. The data collected will not have any personal information associated. You are free to accept or deny this usage. [If accepted, you will be taken to your phone settings in order to change the location access to “Allow all the time”.]”

The disclosure should have both acceptance and denial options. If accepted, only then the permissions requests should be made.



2:27

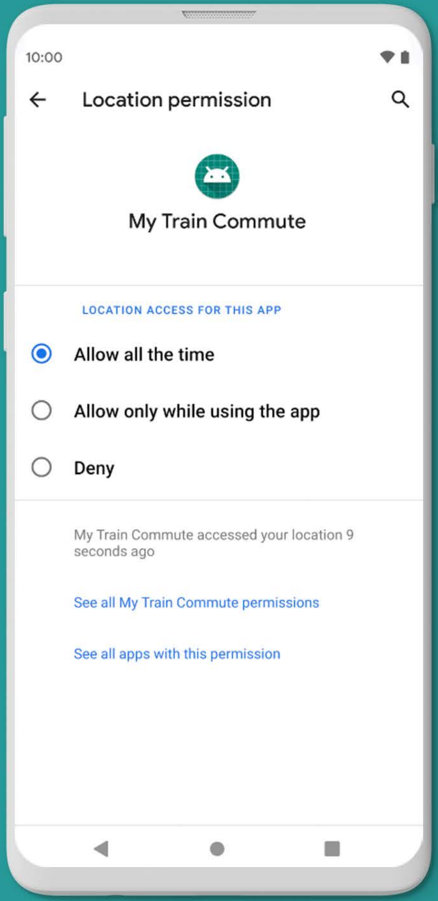
Fri, May 3 1 day, 6 hr

Settings

My Train Commute has been using your location
This app can always access your location. Tap to change.

Manage

Clear all



10:00

Location permission

My Train Commute

LOCATION ACCESS FOR THIS APP

● Allow all the time

○ Allow only while using the app

○ Deny

My Train Commute accessed your location 9 seconds ago

See all My Train Commute permissions

See all apps with this permission

Optimizing Incognia on Android devices

For Android apps having permission for foreground location is a minimum requirement to collect data, having permission for background location provides the best results. Android Apps needing background access have to ask for both <ACCESS_FINE_LOCATION> and <ACCESS_BACKGROUND_LOCATION> permissions. Apps using only foreground access will ask only for the <ACCESS_FINE_LOCATION> permission. Not being able to acquire the <ACCESS_FINE_LOCATION> permission blocks the Incognia SDK from acquiring any location data, while not having the <ACCESS_BACKGROUND_LOCATION> permission only makes it possible to collect it when the application is in the foreground. Using background location allows Incognia to deliver better results for your application.

The Incognia SDK checks the status of these permissions and changes its behavior accordingly. The SDK will work as usual when in the foreground, if only the <ACCESS_FINE_LOCATION> is granted. For further information about adding location permissions to your application, access the explanation for both background and foreground in our open documentation.

03

Best practices on messaging for location permission

Keep in mind that ensuring that users grant location permissions is very important in maximizing the performance of Incognia. The description of why location is used must be clear and provide direct value to the user. If the permission request is hidden or linked to a feature that does not give real value, the acceptance percentage will be small and fewer users will be able to benefit from Incognia services.

Here are examples of messaging for location permissions, that balance transparency, security and articulate clear benefits to the user:

01

“This app uses background location (including geofencing and other location signals) to validate that <insert operation here, such as transaction> was legitimate, according to the user location history. The location data collected is not associated with any other personally identifiable information. Using background location allows the app to reduce friction and improve fraud prevention.”

02

“This app uses location data to provide the location of your purchases, improve fraud security and offer credit product”

03

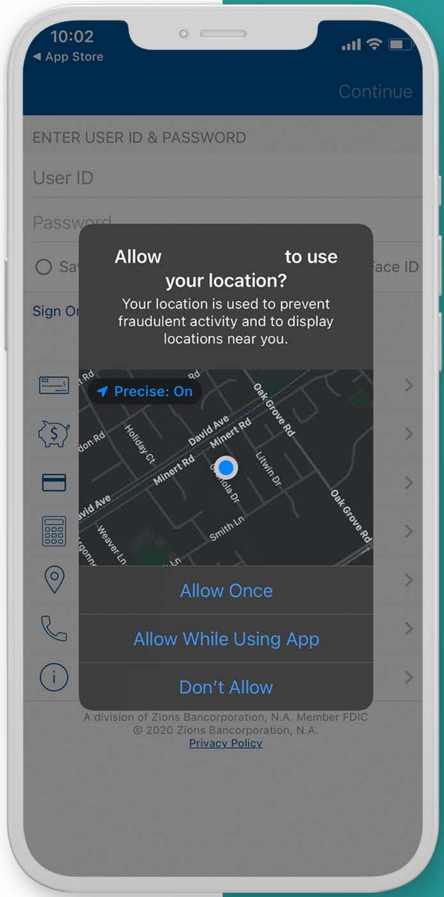
“This app uses location information to improve the security of your in-app transactions.”

04

“We use your location information to improve security against fraud, sending offers, and new products that interest you.”

05

“We use your location information to keep your bank account secure. Do you allow us to access your location information?”



10:02
◂ App Store

Continue

ENTER USER ID & PASSWORD

User ID

Password

○ Sa

ace ID

Sign O

Allow to use your location?

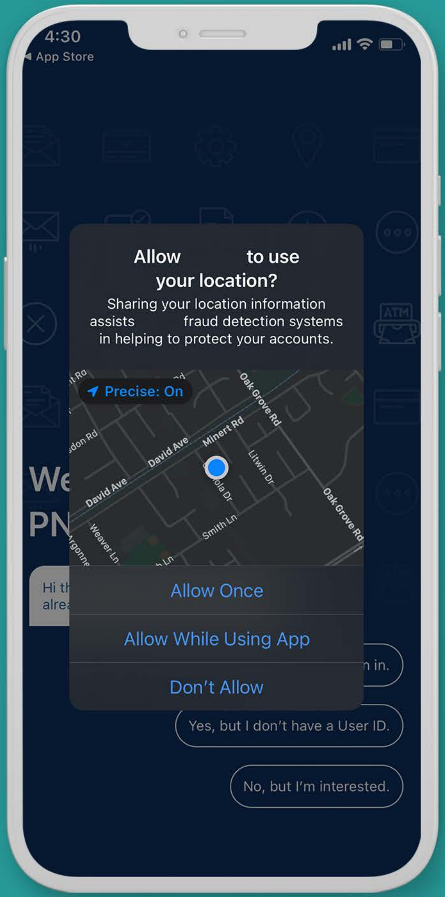
Your location is used to prevent fraudulent activity and to display locations near you.

Allow Once

Allow While Using App

Don’t Allow

A division of Zions Bancorporation, N.A. Member FDIC
© 2020 Zions Bancorporation, N.A.
Privacy Policy



4:30
◂ App Store

Allow to use your location?

Sharing your location information assists fraud detection systems in helping to protect your accounts.

We
PN

Hi th
alre

Allow Once

Allow While Using App

Don’t Allow

n in.

Yes, but I don’t have a User ID.

No, but I’m interested.

Analyzing the types of location permission, it is important to mention that foreground location is essential for Incognia to function and background location is preferred, since it makes it easier for Incognia to identify suspicious behavior in different activities of the user, not only during the in-app interaction.

In addition to having permission to collect location data, it is also necessary that the user has the sensors and network signals switched on for data to be connected. When users turn off cellular, bluetooth and Wi-Fi on their phones, or put the phone in “airplane mode” no data can be detected from those channels. When there is no location data available the Incognia risk-assessment will return with <unknown_risk>, which means that Incognia has no data to return to the app, decreasing the level of security of the user.

Optimum performance checklist

✓ Location Services On
✓ Foreground and Background Permission On
✓ Precise Location On
✓ WiFi On
✓ Cell On
✓ Bluetooth On

Incognia collects location data solely for the purposes of protecting the user and preventing fraud. We do not link location data with any other personally identifiable information on the user such as name, address, SSN. We use extensive anonymization and pseudonymization techniques to encrypt and protect the data we collect to ensure user privacy.

Is there a way for users to opt-out?

Based on privacy regulations, including GDPR, we believe that the user should have control of their data and be given the choice whether to share their location with apps or not, following the guidelines provided by the operating systems. It is important to reinforce that location permissions can help provide a more secure in-app experience, helping to identify cases of identity theft, GPS spoofing and other fraudulent techniques currently being used.

How to know which apps are using location?

Android

Go to settings > Apps >
Apps permissions > Location

iPhone

Go to settings > Privacy >
Location services

04

Device and user identifiers

The Incognia location technology is developed in a way that prevents access to information capable of re-identifying users. Incognia does not collect unique static device identifiers (such as IMEI and MAC), associated accounts (e-mail and telephone), civil identification data (name and social security number), as well as sensitive data (special categories of data) – information that reveals ethnicity, religion, political opinion, religious, philosophical, political or union entities membership or data regarding health, sex life, genetics, and biometrics.

Consent to collect data

Under GDPR - fraud prevention is considered a legitimate interest to collect data. ICO says that "the UK GDPR highlights certain purposes that either 'constitute' a legitimate interest or 'should be regarded as' a legitimate interest." These are:

- Fraud prevention;
- Network and information security; and
- Indicating possible criminal acts or threats to public security.

As further illustration it is a legitimate interest of mobile retailers and financial services to use mechanisms to assist in user identification, fraud prevention and financial crimes. The user has the legitimate expectation that apps will have fraud prevention solutions for validating their registration, preventing theft of their credentials and identifying fraudulent transactions.

When location is used to increase security and prevent fraud, an important question is often asked: "But why would a fraudster, in this case, share their location?" That is one of the reasons why data protection laws, such as LGPD and GDPR emphasize that, when preventing fraud, explicit consent is not necessary, as it is the legitimate interest of the user to remain secure.

Note that although explicit consent is not required, the obligations of transparency and the rights of the data subjects must be observed. So any app should provide information in your privacy policy about the processing of device data by third parties for fraud prevention. activities.

05

How Incognia protects user privacy

Foundational to the Incognia solution is the work we have done to ensure that the location data we collect for the purposes of fraud prevention is treated using extensive anonymization and pseudonymization techniques to encrypt and protect this data. By pseudonymised we mean a security measure in which the personal data can no longer be attributed to a specific data subject without additional information. Such additional information is kept separate and is under technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable person. In addition, Incognia follows five core pillars in its protection of location data and user privacy.

A

We put user privacy first

We follow the 7 fundamental principles of Privacy by Design as the foundation of our product design, implementing privacy protection from conception to final use of our products and solution.

Learn more about privacy by design ⟶

B

We keep location data and individuals separate

We believe the best way to keep individuals and location data separate, is not to collect any data that can directly link to identity. At Incognia we focus on encrypting and protecting the location data we collect, and intentionally do not collect any additional PII from the users of a mobile app. We do not need to, or want to know the real world identity of any user.

If you would like to learn more about how we treat data and privacy please review our privacy policy.

Review our privacy policy ⟶

C

We handle special category data with extra care

Incognia technology immediately classifies collected data as sensitive, strips it of identifiers and stores it as a visit to “special category[2] - place A”, because it is sensitive. Without information on the individual, context on the place or linkages to other location data, the information becomes anonymous, and the privacy of that user is protected.

D

We use proprietary location anonymization and pseudonymisation technology

We focus on hashing and encryption to protect the location data we collect, and intentionally do not collect additional PII. Other techniques we use include probabilistic set structure, differential privacy, and k-anonymity, bringing the data closer to full anonymization.

E

We are mindful of data retention

Just because data can be kept, doesn’t mean it should be. At Incognia we follow the best practice of only keeping data as long as it is actively used. If data isn’t stored, it can’t be stolen or contribute to downstream fraud caused by stolen credentials and PII.

[2] Information Commissioner’s Office

Key takeaways

01

Operating Systems are increasing their controls on the use of location data and all apps should follow legal basis to ask for location permission.

02

There are different methods of collecting location data and asking for permission

03

Incognia is compliant with LGPD/GDPR/CCPA and the obligations of transparency to the user

04

There is a way for users to opt-out from location permissions.

Contact us to know more about adding Incognia device and location behavior intelligence to your mobile app to reduce friction and fraud, respecting privacy, recognizing trusted users in real-time, and driving increased mobile revenue.

Contact us ⟶

Understand more about our location identity for mobile, and our privacy policies and know more about how Incognia deals with privacy

Access privacy policies ⟶

Learn more about privacy ⟶

For further information, read our developer docs. To understand best practices on how to add location permission to your app: Android, for both background and foreground iOS

Android ⟶

Background Android ⟶

Foreground Android ⟶

iOS ⟶

Read more

How-to Series

Location Technology: Build vs. Buy

5 Important considerations

Learn more ⟶

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 costs throughout the customer journey. Incognia's award-winning technology uses location signals and motion sensors to silently recognize trusted users based on their unique behavior patterns. Deployed in over 100 million devices, Incognia delivers a highly precise risk signal with extremely low false positive rates.

INCOGNIA™