

How-to Series

Understanding Incognia Location Identity

5 Key Location Technology Concepts



Incognia has spent the last nine years developing its proprietary location technology, which uses mobile sensor data to build an anonymous location behavior pattern unique for each user that creates a private digital identity - like a location fingerprint.

Outlined in this ebook are the key location concepts used by Incognia to enable location as the strongest trust signal on mobile and its use for mobile authentication and fraud prevention.

How does Incognia build a location identity?

Today's smartphones contain a number of sensors that provide location information. These sensors include GPS, Wi-Fi, Cellular, and Bluetooth in addition to motion sensors. Incognia uses these location and motion sensors to deliver highly precise location information that is resistant to spoofing and that forms the basis for a private digital identity based on user location behavior.

The most widely known geolocation technology is GPS however this is now very typically spoofed, meaning that fraudsters can easily fake their location to fool GPS sensors. For this reason Incognia makes use of not only GPS but also Wifi, Cellular and Bluetooth sensor data.

Understanding on-device location sensors



GPS - Global Positioning System

GPS is the most widely used form of geolocation technology used on mobile devices and is also now regularly spoofed. GPS geolocation is based on communication satellites that orbit the earth, that continuously broadcast their status, exact location, and precise time. A GPS device that receives these signals is able to determine its GPS location. The accuracy of the GPS location is based on several factors including atmospheric conditions, signal blockage, and receiver design and quality, and it is between near 33 to 330 feet.

There are multiple techniques that fraudsters routinely use to spoof location, including GPS spoofing apps, VPNs, Proxies, and emulators.

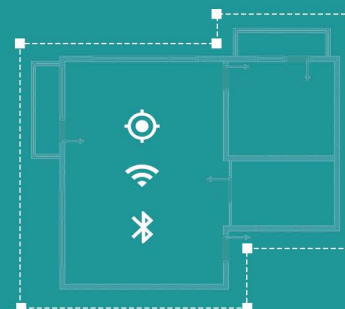


Wi-Fi

For Incognia, Wi-Fi provides important location sensor data. Wi-Fi positioning, known as WPS or WiPS, is based on Wi-Fi hotspots and wireless access points. The most common method for geolocation is based on measuring the receiving signal strength - known as the Received Signal Strength Indicator (RSSI) from a number of Wi-Fi hotspots or access points. Wi-Fi positioning is particularly useful for indoor positioning where GPS does not perform well.

Incognia detects and identifies Wi-Fi networks and assesses reputation and scale, adding this information to our network data, so we can check the correlation between locations, devices and fraudulent activities such as fraud farms.

In addition to Wi-Fi, Incognia location technology also makes use of Cellular and Bluetooth.



Location mapping

GPS coordinates, Wifi & Bluetooth signals are bundled to create a location environment



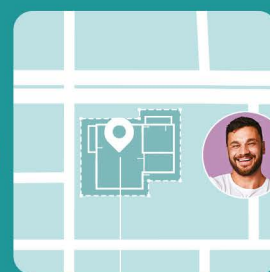
Crowdsourced updates

Location environments are strengthened and updated each time an Incognia device visits



Competing technology

Less precise



Incognia's technology

Higher accuracy, even indoors

Unparalleled accuracy

Incognia's innovative approach to location generates very low false positive rates, **below 0.0013%**



Cellular

Cellular networks are enabled by a network of cell towers that transmit the radio-waves that are used for mobile communication. Similar to how satellite signal broadcasts are used to locate a device, cell tower signals can also be used for geolocation, although this method is not as accurate as GPS, typically only accurate to within an area of 0.75 miles.




Bluetooth

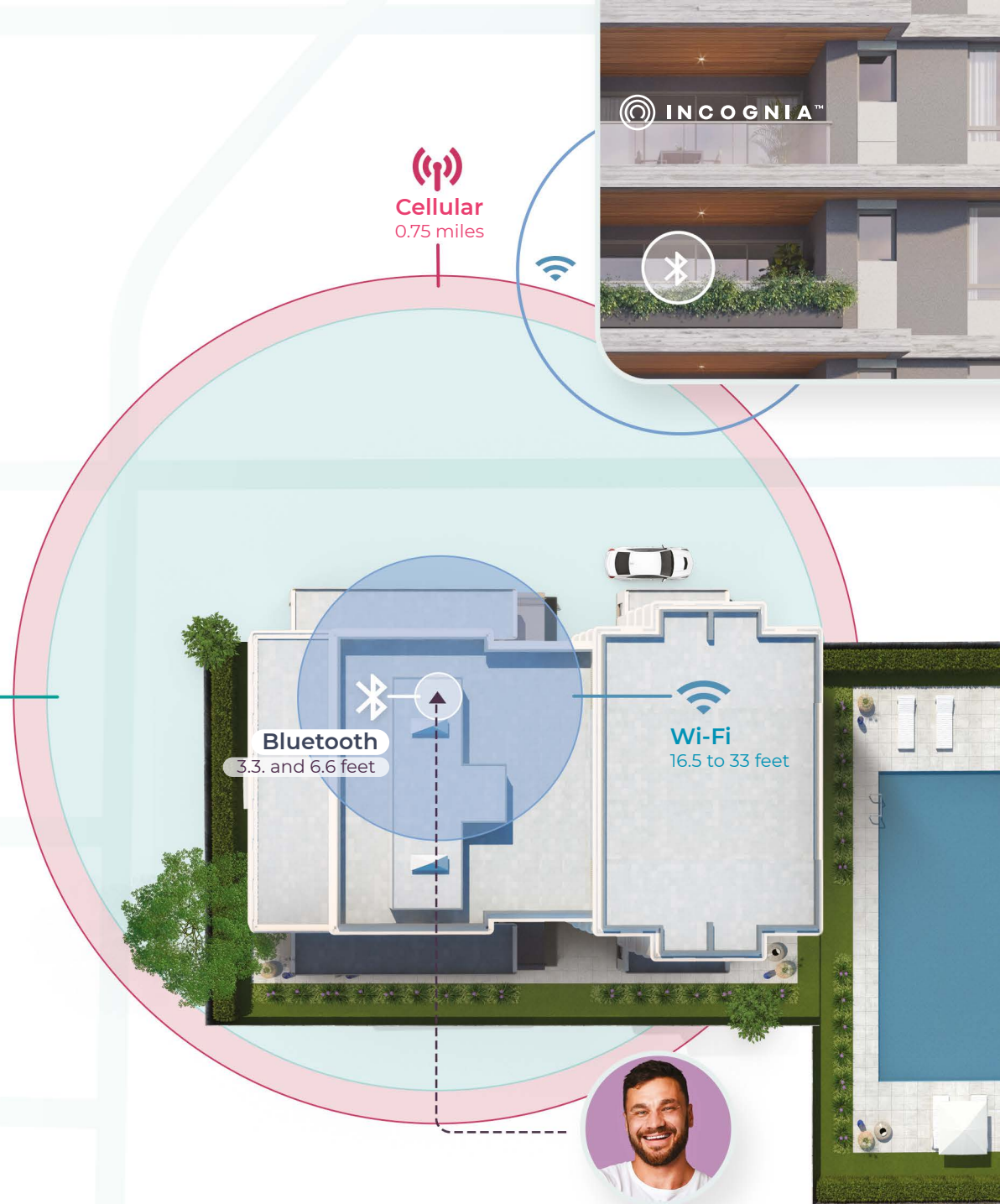
Bluetooth is a wireless technology used for communicating short distances over short wavelength radio waves between devices, with an accuracy between 1 and 2 meters. The most recent version called Bluetooth Low Energy (BLE) is built into many smartphones. Smartphones can determine their location based on picking up signals from BLE beacons enabling an indoor positioning system.


GPS
33 to 330 feet
Accuracy


Cellular
0.75 miles


Bluetooth
3.3 and 6.6 feet


Wi-Fi
16.5 to 33 feet



Understanding Key Location Behavior Concepts

Using the location sensor data from the device, Incognia uses a number of key location behavior concepts to create Incognia's location identity for mobile authentication and fraud prevention.

01

Environments

Incognia location technology is based on the concept of environments. Each location has a unique signature of GPS coordinates, and available Wi-Fi, Bluetooth, and cellular network signals. Incognia maps and correlates these signatures to create unique environments and uses this information to identify the location of a device with high precision and accuracy, even indoors. Unlike fraud solutions relying solely on GPS, which can be easily spoofed, Incognia's approach to location is highly resistant to location spoofing and effective in detecting those techniques.

02

Location Fingerprint

Each user has a unique location behavior pattern, like a location fingerprint, that comprises frequently visited locations specific to that user. As the user moves location this location fingerprint is constantly changing and updating making it extremely difficult to mimic or forge.

03

Trusted Locations

The highly frequented locations by the user and device are classified as the user's trusted locations. When Incognia detects a user is in a trusted location, there is a higher probability of the transaction being legitimate and at lower risk for fraud, offering the opportunity of a frictionless authentication experience.

04

Location Detection

Incognia uses geofencing and activity recognition techniques to detect if a device has significantly displaced its position. Recognizing this movement allows Incognia to preserve battery life by only collecting location events that matter, mainly at the moment when a device arrives or departs a particular location. By scanning Wi-Fi and Bluetooth signals, Incognia can detect displacements in position and confirm that the device is at a different location, or returning to an already mapped location without having to pull GPS coordinates every time. In this way, Incognia minimizes battery consumption on the device to 0.5% in 24 hours.

05

Behavior Watchlist

The Incognia technology is deployed in over 100 million devices providing a powerful network effect. Devices and locations that have been associated with fraud or suspicious behaviors are added to the Incognia Behavior Watchlist. As a customer of Incognia, any device or location on the watchlist will be indicated in the evidence list. This information will be used in the risk assessment.

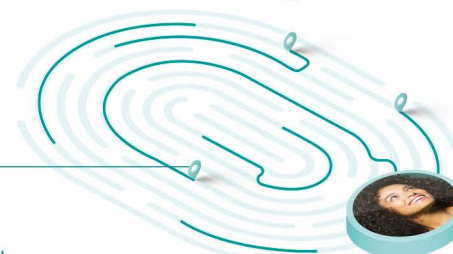
Behavior Watchlist



Trusted Locations



Location Fingerprint



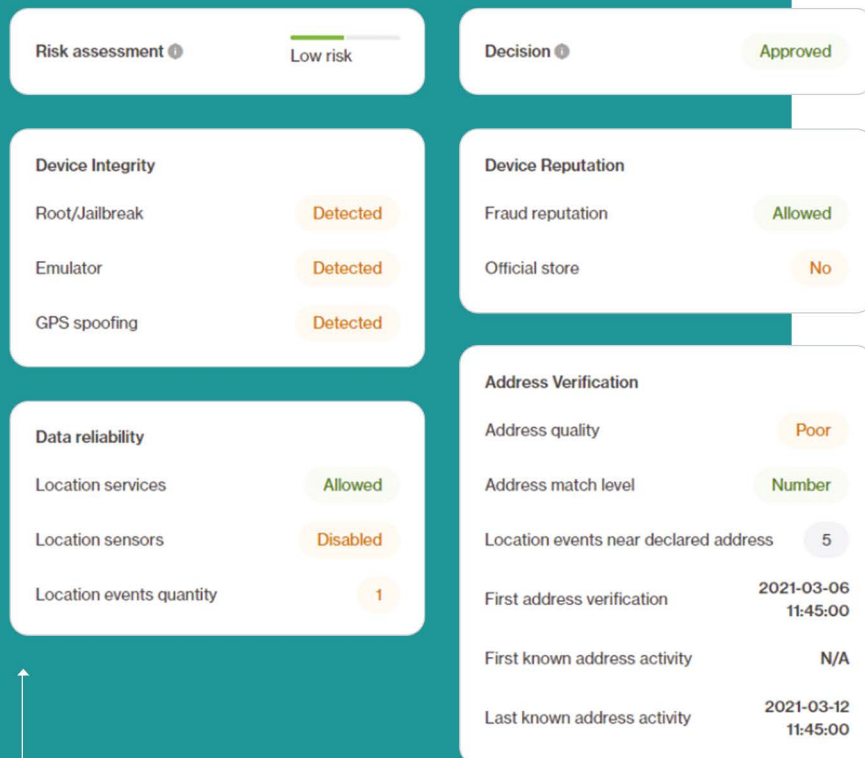
Location Detection

Environments



Incognia Location Identity Solution

The Incognia location identity solution comprises a mobile SDK that collects location sensor data from the device and also an API that provides a risk assessment based on the data. Here is an example of the risk-based authentication process using the Incognia SDK and transaction API and an example evidence list.



01

The user accesses the app and logs in



02

The incognia SDK collects the user location at the moment of the authentication



03

The risk engine calls the Incognia API

First call - Checklist

- Is it a compromised device?
- Is this device our watchlist?
- Is there systemic fraud behavior, such as creating multiple accounts from one device?

Device integrity and device reputation

Detection of anomalies: root/jailbreak, emulator, app was downloaded from official store

Fake location detection - GPS spoofing

Second call - checklist

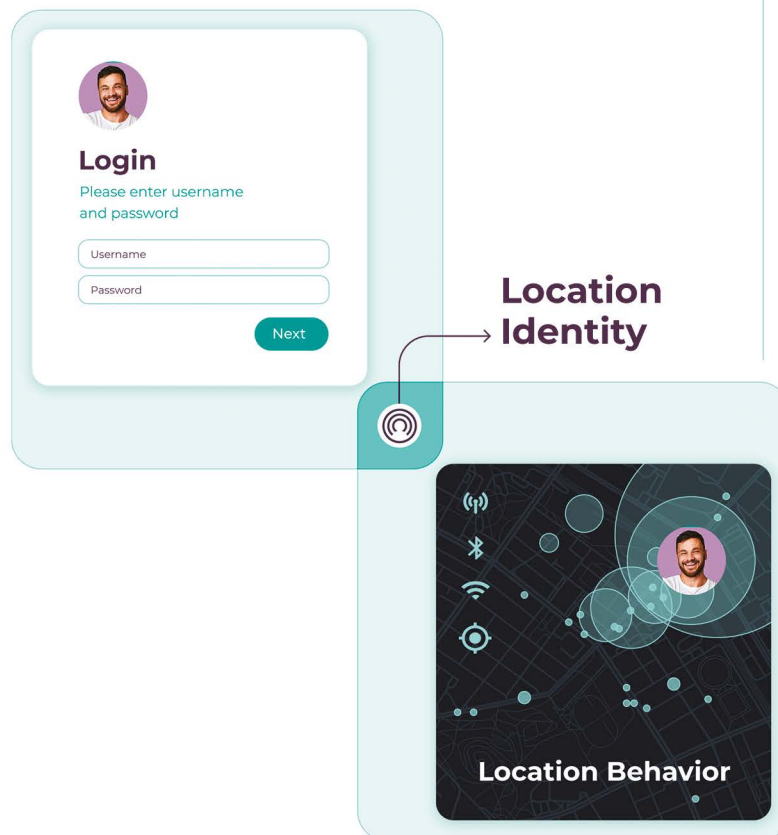
- Is the login attempt occurring from a trusted location or nearby?
- Is this trusted location related to the user location fingerprint?

04

The Incognia API delivers a risk-score based on the Incognia evidence list

Authentication

The Incognia risk-based evidence list considers key information about device integrity, device reputation, location behavior and location sensor data.



Evidence list detailed view:

Risk assessments

High risk

Decision

Denied

Device Integrity

Root/Jailbreak

Not detected Detected

Emulator

Not detected Detected

GPS spoofing

Not detected Detected

Device Reputation

Behavior reputation

Suspect Unknown Allowed

Fraud reputation

Confirmed fraud Unknown Allowed

Official store

No Yes

Location Behavior

Distance from trusted location

331 feet

Last location timestamp

2021-03-03 18:11:16

Location sensors

Sensor match type

GPS WiFi scan WiFi connection

Data reliability

Location services

Denied Allowed

Location sensors

Disabled Enabled

90%

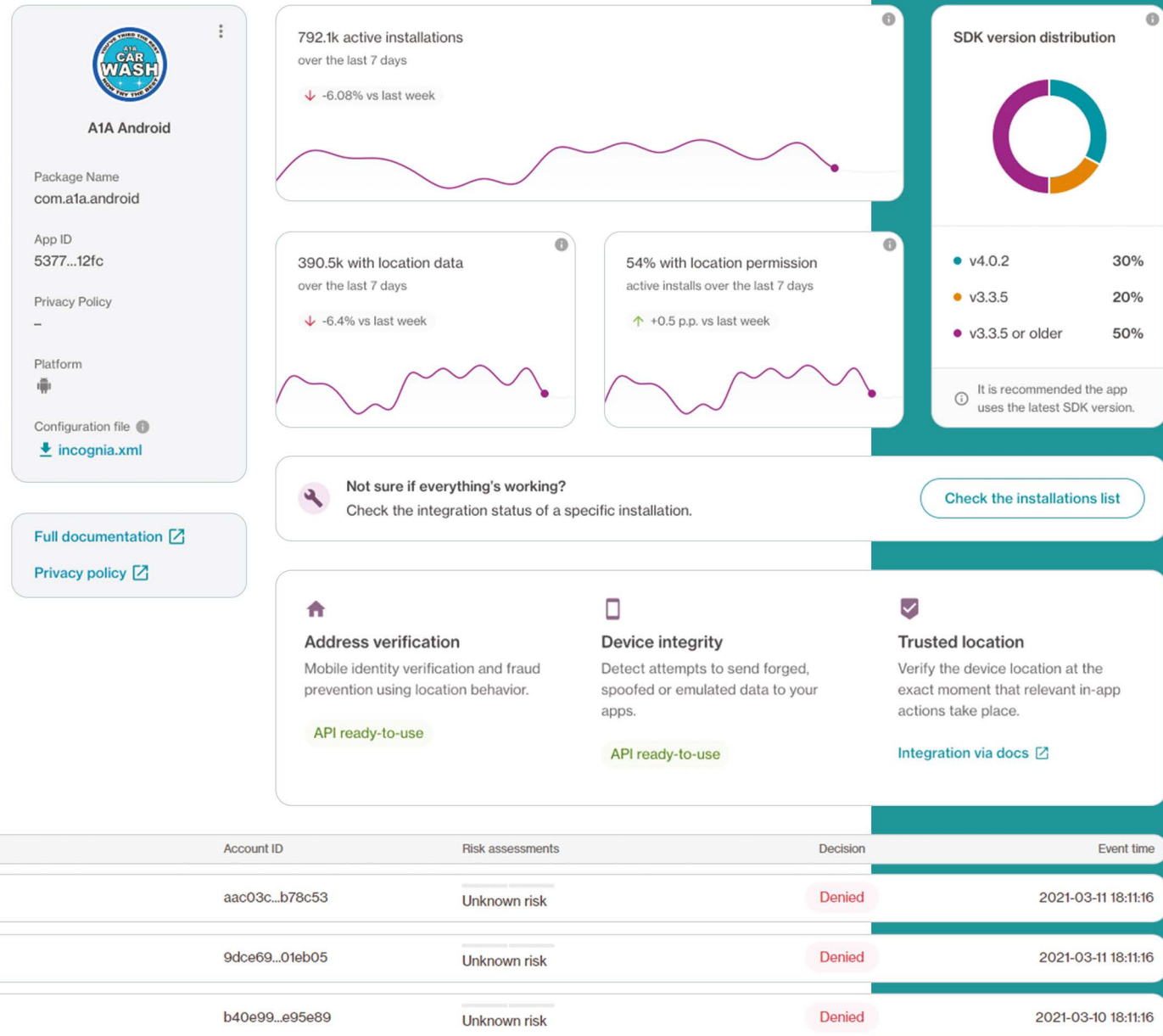
of legitimate logins happen from Trusted Locations such as home

95%

of sensitive transactions that are not fraudulent happen from Trusted Locations

Evidence list overview:

Incognia explains the status of your application including the user base, opt-in rate and the result of the risk assessment for each login ID.



Location permissions

The Incognia SDK detects location points and collects location data solely to protect the user and to prevent fraud. For optimum performance Incognia relies on the following device features and permissions:



Location services
should be turned on



The mobile device should be
connected to a network



The user should provide their
permission to collect location data

Mobile users that do not provide their location permissions, and do not have their location turned on, will not generate location data, thus, are not able to benefit from our features. The Incognia location identity solution is most effective when as many users as possible allow the use of the location. We typically see high rates of user opt-in (80% or more) when the user clearly understands the purpose for location permissions. For more information on how to request location permissions read more in our ebook: [Location Permissions - 5 Important Considerations](#).

Our privacy-first approach to location

Location data can easily become very sensitive. That's why Incognia follows Privacy by Design in the development of our solution and we intentionally do not capture, store or associate any additional PII with location data. We provide special treatment to visit data associated with sensitive locations, such as religious temples, hospitals and others. We focus on hashing and encryption to protect the location data we collect, and other techniques we use include probabilistic set structure, differential privacy, and k-anonymity, bringing the data closer to full anonymization. For more information on Incognia's commitment to privacy read more in our ebook: [Privacy by Design](#).

Key Takeaways

- Location sensors provide behavioral signals that are hard to mimic or forge.
- Location provides a strong trust signal on mobile.
- The Incognia location identity solution comprises a mobile SDK that collects sensor data and also an API that provides a risk assessment based on the data.
- GPS is only one element of what is needed to build a location technology that can beat fraud.
- Incognia uses five key location concepts to deliver highly precise risk scoring: trusted locations, location fingerprints, environments, location detection and behavior watchlist.

[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.

Understand more about considerations behind developing or adopting a location technology solution read How-To Series: [Location Technology - Build vs. Buy](#)

Further reading

How-to Series

Location Permissions
5 Important Considerations

Learn more →

How-to-Series

Location Technology
Build vs. Buy

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.



© 2021 Incognia All Rights Reserved