How-to Series

Location Technology - Build vs. Buy

5 Important Considerations

INCOGNIA™

Outlined in this document are five important factors to consider when evaluating location technology and whether to build vs. buy.

When a company identifies a new software need, there are two options, either build in-house or buy an existing solution. Internal teams are often drawn to the idea that a homegrown solution can be built to fit the exact specifications needed and connect seamlessly with existing systems, however building in-house comes with the cost of development, upkeep and maintenance.

01

Understanding location technologies

Incognia has spent the last nine years developing its proprietary location technology which makes use of sensor signals on the mobile device including GPS, WiFi, Bluetooth to deliver highly precise location information. Every location has a unique set of signals captured by these sensors, and Incognia maps these signatures to unique environments 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 effective at detecting location spoofing.

Location Spoofing - Common Techniques

Today, fraudsters use a number of techniques and off-the-shelf tools to routinely spoof location and fool fraud prevention systems using location models based on GPS and IP addresses.

VPNs and Proxies hide the user's IP address through connection with a remote computer and thereby conceal the user's true location.

GPS Spoofing Apps have become widely used due to location-based massively multiplayer online role-playing games (MMORPGs), GPS spoofing apps can be easily configured on mobile devices to activate GPS spoofing.

Mobile emulators are a standard tool used by developers to test mobile apps. One of the data points that is easily manipulated via a mobile emulator is geolocation information.

Instrumentation tools such as Frida, are used to mimic a device, and spoof location to fool fraud prevention systems.

App tampering is also a technique used to insert custom code to report fake locations.

> Incognia’s technology uses network signals and motion sensors to provide highly accurate location behavior intelligence that is extremely difficult to spoof.

Location Detection

Another major consideration with using geolocation technologies is that sensors, such as GPS, consume a lot of energy, draining the device’s battery quickly if misused. For mobile apps using background location, Incognia uses geofencing and activity recognition techniques to recognize if a device has moved significantly, enabling the identification of the moment when a device arrives or departs a particular location. In this way, Incognia minimizes battery consumption on the device to 0.5% in 24 hours. By scanning Wi-Fi and Bluetooth signals, Incognia can detect displacements in position and confirm that the device is at a different location. The incognia SDK dynamically changes the frequency and mechanics used for consulting each sensor according to several factors, ranging from the time of the day, to the model and brand of the device and its components. Incognia performs this type of optimization continuously, including every time a new mobile operating system version or update is published, or new device hardware is released.

02

Continuous upkeep, maintenance and development

Incognia has a team of more than 90 full-time engineers that has focused on building and optimizing our location stack for the past decade. This represents a substantial amount of development time and accumulated knowledge applied to the continuous optimization of our solution. An in-house development effort would demand significant effort to reproduce and maintain a solution such as Incognia. Our proprietary location technology includes mechanisms for optimizing the capture of location information and understanding its context.

Learn How Incognia Works ⟶

The iOS and Android platforms are constantly evolving and being updated, which means frequent changes in how each OS treats access to sensor data, and management of user consent. This is a constant development effort to keep up-to-date with mobile devices and their systems changing on a daily basis. Incognia has in-house SDK teams for each OS and they are constantly monitoring, researching, and optimizing our location stack to the latest versions of operating systems and devices.

Recording and treating location data from millions of devices every day requires extensive computing power and cloud storage space, not to mention applying the required security and privacy techniques that are complex and always evolving. Incognia has a team that is constantly maintaining and optimizing cloud usage of its platform and making continuous improvements. We focus on keeping cloud storage and computing power consumption to a minimum while maintaining response times for data retrieval at its highest for achieving optimal costs with the best performance.

Quick SDK & API integration

Mobile SDK

Easy integration wizard

Integration time: 1 hour

SDK weight: 415 KB (Android)
1.5 MB (iOS)

Battery usage: ~0.5% per day

APIs & Webhook

REST & JSON Response

Average response time: 60 ms

Availability: 99.76%

03

Development and time-to-market

Using a ready-to-go solution instead of developing internally accelerates time-to-market and minimizes opportunity cost. By opportunity cost, we mean the growth and revenue lost while developing an internal solution, rather than implementing a comprehensive solution right away.

Incognia's near-decade of experience working with global customers and hundreds of mobile apps of all sizes and categories, provides us with expertise in industry best practices, benchmarking across market segments, technical implementation and user experience flow. Our customer success, product, and privacy teams are ready to share this experience to support our customers in implementing the best approaches for ensuring optimized customer experience, best practices for user opt-in for sharing their location, and considerations for regulatory data privacy compliance.

04

Privacy and data governance considerations

Incognia follows Privacy by Design principles, ensuring that privacy is central to our product strategy from concept to product launch. We have a team dedicated to ensuring that the location data we collect is encrypted, anonymized and never linked to any individual person and their PII. We intentionally do not collect, store or process any additional personally identifiable information, including names, e-mail addresses, phone numbers, government-issued IDs of mobile app users. All sensitive data remains at our customers' servers, meaning that Incognia never has access to this kind of data.

In addition, we do not collect data from visits to sensitive places such as religious temples, hospitals, political parties, places of adult entertainment, and other location that might be used for making sensitive inferences of information such as ethnicity, religion, political or philosophical opinion, union membership or data regarding health, sex life, genetics, and biometrics.

Incognia follows five core pillars in its protection of location data and user privacy, which are:

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 sensitive special category data place visits with extra care

Incognia technology immediately classifies collected data as sensitive, strips it of identifiers and stores it as a visit to “special category - 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.

05

Network effect

To date Incognia's location technology has been deployed in more than 100 million mobile devices which provides us with knowledge from a much larger user-base than most individual apps would be able to get standalone. This knowledge and experience enables incognia to deliver improved reliability, accuracy, and efficiency of the solution, benefiting all parties involved. Some of the network effect benefits include a better database of places, classification algorithms which are fed by A.I. that learn and get better over time, immediate recognition of users and their trusted locations, better decisions for corner cases and an improved Incognia watchlist for fraud detection.

Location technology perfected over a decade now powers Incognia's location identity solution. Location gives us the power to match digital and physical identities for real-time address verification, compare location behavior to detect Account Takeover, and secure mobile and in-store contactless payments. Our mission is to protect mobile users throughout their digital journey.

Read more

How-to Series

5 Things to Know About Location Permissions for Fraud Prevention

Learn more ⟶

Infographic

Understanding smartphone location technology

Read the infographic ⟶

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™