Kingsmead Security Ltd

Enhancing Geolocation for Cutting-Edge Streaming Services

Kingsmead Security Whitepaper

Executive Summary

Geolocation solutions are required for streaming services to meet their business, contractual and legal obligations. In contemporary services, IP-based geolocation is universally deployed. The use of more sophisticated geolocation technologies remains rare.

However, IP-based geolocation can be inaccurate by 100km+ and accuracy degrades further for some types of networks (for example, cellular or satellite networks). In addition, VPNs are increasingly used by users to evade geo-restrictions and conceal their true location. Streaming operators deploy VPN detection solutions to block VPN usage, but performance can be low for many of them due to the use of proxy networks by VPN vendors.

IP-based geolocation and VPN detection remain important, but more robust methods are increasingly required to meet current requirements and to enable new products and services.

This whitepaper discusses the pros and cons of current methods and suggests future geolocation methods. Increased use of accurate device-based location services is likely to be inevitable, but the impact on consumers and their privacy must be addressed.

Copyright © 2026 Kingsmead Security Ltd. All rights reserved.

Key Questions

Q: Who should read this whitepaper?

This whitepaper is aimed at streaming operators and content owners, and is essential reading for both technical teams and product owners.

Q: Why do streaming operators require accurate geolocation?

Geolocation is required to meet content licensing requirements, especially sports content rights which may have regional geolocation requirements. In addition, streaming operators must adhere to local government regulations (for example, EU Content Portability).

Aside from contractual and legal requirements, geolocation is required to configure services for each local market (localisation), to manage customer experience and to manage malicious activity.

Q: What are the primary risks to streaming operators of inaccurate geolocation?

Failure to meet geo-restriction requirements in content licensing agreements risks future content availability and complicates future licensing negotiations. Failure to meet local regulations may lead to fines and reputational harm.

Q: Does IP-based geolocation meet industry goals?

IP-based geolocation is the standard method for geolocation in streaming services. It is widely available, easy to deploy, cost-effective, efficient and unintrusive for the user. However, fine-grained geolocation accuracy can be poor, and accuracy degrades further on cellular or satellite networks. IP-based geolocation can be faked using VPNs and other anonymising services which are now widely used by consumers. Consumer privacy networks such as iCloud Private Relay can also be used to mask location.

Q: Are more sophisticated geolocation solutions available?

Many modern consumer devices have built-in location services which a streaming service can use to confirm a user's location. Location services use a range of data sources to detect geolocation, including GPS, Wifi, cell towers and Bluetooth. When used in combination with other device information, an extremely accurate location can be identified.

Q: What new opportunities can accurate geolocation bring streaming operators?

Accurate fine-grained geolocation not only ensures robust contractual and legal compliance but enables new opportunities for streaming operators. For example, new content licensing deals can be developed, based on accurate regional or even city-level geolocation. Highly localised advertising or content recommendations can also be developed.

On a more practical level, if a trusted geolocation is available, operators may be able to relax signup rules which require local payment methods or local cellphones, which can block some legitimate customers.

Q: What challenges could streaming operators face when deploying more sophisticated geolocation solutions?

Streaming operators need to ensure that their geolocation technology is available across all device types and is robust to tampering. Streaming operators should also ensure that they sensitively handle consumer concerns around privacy.

Q: Are sophisticated geolocation solutions already deployed?

A number of streaming services have already deployed more sophisticated geolocation solutions in their services, and more services are planning to do so. Regional content licensing deals, especially sports content, is driving many of these developments.

Copyright © 2026 Kingsmead Security Ltd. All rights reserved.

1 Introduction

All streaming services available today need to identify a user's geolocation in order to manage their service and customer experience. Geolocation is often perceived primarily as a method to geo-restrict services to meet content licensing and legal requirements, but other requirements apply. We'll explore in more detail some of these requirements in Section 2.

In traditional broadcast networks, there is a physical constraint to geographic coverage:

- Cable networks are wired directly to homes.
- Terrestrial towers broadcast to areas up to around 100 km of the tower.
- Satellites broadcast into a large geographic area but could be restricted via distribution of physical STBs or smartcards.

When streaming "over-the-top" (OTT), there are no physical barriers. The Internet was designed without physical boundaries and without centralised control. This means that geolocation for OTT services can be challenging.

The streaming industry currently uses IP-based geolocation to manage its customer base. This is discussed in Section 3. However, IP-based geolocation can be inaccurate by 100+ km, and the increased use of cellular and satellite connectivity further weakens IP-based geolocation. Consumers are also using VPN services and more advanced location masking technologies to bypass the geo-restrictions of streaming services.

For many services, deploying IP-based geolocation with VPN detection has mixed success. Many VPN vendors can almost guarantee access to any streaming service they choose to target. Worse, inaccurate geolocation can mistakenly block users, and VPN use can degrade service levels. This potentially leads to customer dissatisfaction and possible revenue loss for operators.

As the streaming industry matures, a new approach needs to be considered. Section 4 discusses the use of device-based location services for accurate fine-grained geolocation. Consumer applications in other industry sectors use these more advanced location services to improve the customer experience, but this is still rare in the streaming industry.

2 Why Geolocate?

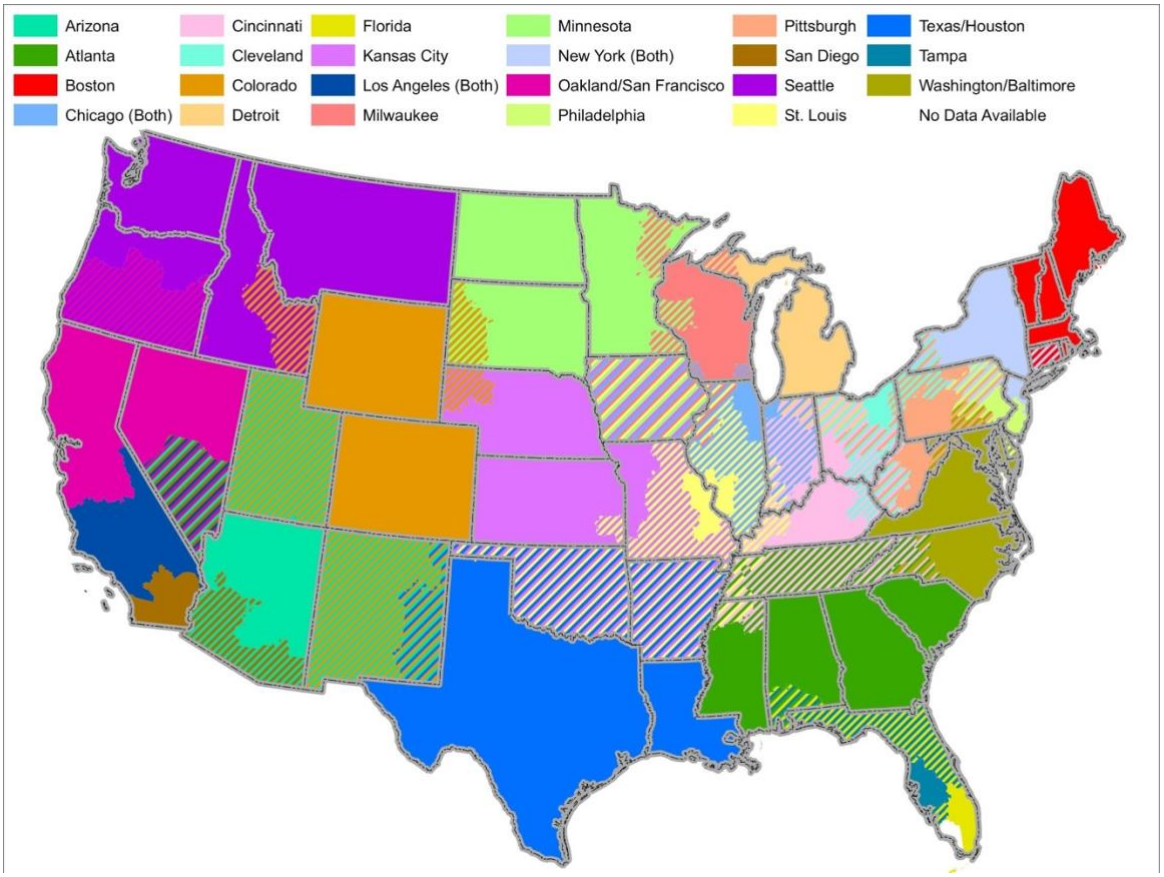
This section discusses the reasons why streaming services require geolocation. Requirements will vary across services and countries – there is no one-size-fits-all.

Enforcing Content Licensing Requirements

The primary reason for many streaming services to geolocate users is due to content licensing requirements. Studios and sports leagues license content to specific streaming operators to allow local distribution with local packaging and pricing policies. For example, English Premier League soccer is considerably more valuable in the UK compared to other countries.

Most content licensing deals require country level geo-restriction. However, some deals require region/state level geo-restriction, or even more fine-grained geo-restriction. For example, city level local blackouts are often required for sports content (e.g. the NFL, MLB and NHL in the US). The MLB blackout map in the US is illustrated below:

Copyright © 2026 Kingsmead Security Ltd. All rights reserved.



US MLB Blackout Map (Image credit: Wikipedia)

Enforcing these blackouts requires highly accurate fine-grained geolocation.

Failure to meet geo-restriction requirements in content licensing agreements risks future content availability and complicates future licensing negotiations. In addition, poor geo-restriction may lead to tension with other streaming operators if content leaks into their operational territory.

Legal Requirements

Legal requirements also need to be met by streaming operators. This includes regulations such as:

- EU Content Portability – Content purchased in one EU country must be accessible whilst travelling in other EU countries.
- Local Content Censorship – Content may require specific editorial changes to meet local regulation (e.g. offensive material).
- Content Ratings – Local content ratings may apply (content labelling, age ratings, rating enforcement, etc).
- Advertising Rules – Local rules around advertising may be enforced in some countries (e.g. no unhealthy food ads before 9pm).

Failure to meet legal requirements may lead to fines and reputational damage for streaming operators.

Localisation

Many streaming operators span countries, and they need to manage their service accordingly. Streaming services can vary a great deal across countries, even within the same brand:

- Content availability, versioning and packaging.
- Currency and pricing configuration.
- User interface language configuration.
- Default language settings during content playback.
- Local sign-up preferences (email, cellphone, etc).

Copyright © 2026 Kingsmead Security Ltd. All rights reserved.

- Local payment mechanisms.

Managing Customer Experience

Streaming operators aim to deliver an excellent service to their users. Unhappy users cancel their service or drive support costs. Legitimate customers will be lost if they are blocked due to inaccurate geolocation.

User experience may also be disrupted if VPNs are used (playback errors, buffering, low resolution, etc.). Detecting VPN use allows operators to manage the user experience more effectively.

Managing Malicious Activity

Any service on the Internet is a potential target for a cyber-security attack. This is an ever-present risk for everyone, and all services should protect themselves as much as possible. For streaming services, the additional risk of content piracy is a constant threat to the industry.

Applying robust geo-restriction, malicious IP detection and VPN detection can reduce the attack surface of a service. If these measures are not introduced, an attacker can more easily evade detection. Further, a streaming operator may have limited opportunities for legal action if attacks can take place from countries with limited enforcement options.

There are various types of malicious activity that a streaming operator may be concerned with:

- Credential Sharing – Users are often tempted to share their credentials with family and friends in order to spread costs. Accurate geolocation enables more accurate detection of this activity, leading to new revenue opportunities for the streaming operators via service add-ons or new subscribers.
- Unauthorised Users – Users may avoid geo-restrictions to gain access to content and services not available to them. These consumers are often frustrated consumers unable to access content or seeking better value.
- Fraud – Users may sign-up for services fraudulently, using fake or stolen identities and payment methods. Alternatively, fraudulent streaming services may resell access to legitimate services in other countries.
- Piracy – The illegal download and distribution of copyrighted works remains a major threat to the industry. Piracy is a breach of the law and may lead to criminal action.
- Cyberattacks – Cyber-attackers often hide their activity through the use of VPNs and other techniques. Attacks vary from credential stuffing attacks to service reverse-engineering for the construction of pirate scripts.

These impact streaming operators in different ways depending on their operational territory and the type of service they offer. A sensible approach to managing these risks is required.

New Product Opportunities

The streaming market is changing. Traditional distribution models are evolving to meet the needs of a streaming world. Accurate geolocation is required to deliver many of these new opportunities.

For example, the traditional model of licensing sports content to Regional Sports Networks (RSNs) in the US is changing. Increased cord cutting, increasing licensing costs and an increasingly fragmented industry has undermined the traditional RSN model. Some sports rights are moving to national networks, but new opportunities are also evolving at the local level. The evolving market has enabled local teams to build their own streaming services and serve their fan base directly.

Another example of the changing sports licensing market comes from Australia. The 2025 AFL season introduced a new broadcast rights deal which introduced free-to-air games on streaming for the first time[1]. In order to meet the requirements of the deal, streaming operators were required to accurately target games to home markets. This introduced an increased accuracy and spoofing detection requirement for geolocation.

[1] https://www.afl.com.au/news/837244/afl-reveals-new-broadcast-rights-deal-from-2025

Copyright © 2026 Kingsmead Security Ltd. All rights reserved.

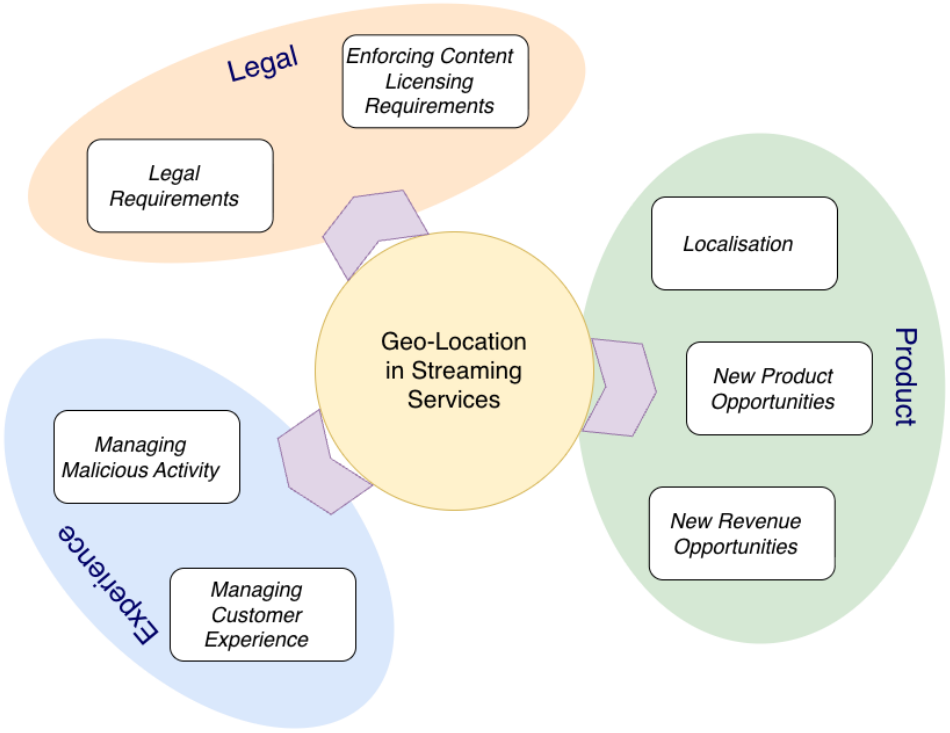
New Revenue Opportunities

Accurate geolocation potentially unlocks new revenue opportunities for streaming operators. For example:

- Location-based targeted content recommendations and upsell opportunities.
- Location-based targeted ads allowing highly localised advertising.
- Better enforcement of commercial premises vs residential consumer contracts (for example, bars and restaurants).
- Ability to offer 'exclusive' content for users in-venue (for example, in a stadium).
- Ability to accurately control distribution of content across regions within a country.

Summary

Although content licensing requirements are often cited as a major driver for geolocation in streaming, there are many other product and legal requirements which require accurate geolocation. As the industry continues to evolve, we're seeing more streaming operators exploring fine-grained geolocation to drive new product innovation and revenue opportunities.



3 IP-Based Geolocation

IP-based geolocation is the standard method for configuring streaming services. All streaming services are expected to use IP geolocation as part of their service.

Advantages

IP-based geolocation is widely available, easy to deploy, cost-effective, efficient and unintrusive for the user.

Disadvantages

Fine-Grained Geolocation Accuracy Poor

No-one knows the precise geolocation of all IP addresses on the Internet. The Internet wasn't designed that way and is constantly evolving. IP geolocation vendors use a variety of techniques to geo-locate IP addresses, but accuracy can vary across vendors, countries, IP address type (residential, mobile, data centre, etc), ISPs and other factors.

Most vendors claim around 99% accuracy for geo-locating IP addresses to countries. For services requiring geolocation to the country level, this is an acceptable performance level. For services requiring state or city level geolocation (such as enforcing sports blackouts to city, state or other boundaries), accuracy very quickly degrades to a level which is unacceptable.

Copyright © 2026 Kingsmead Security Ltd. All rights reserved.

Cellular/Satellite Network Geolocation Accuracy Poor

In recent years, 5G cellular networks and satellite Internet services have become more accessible to consumers. These services are used both inside and outside the home. As these services continue to grow, costs will fall and bandwidth will increase, potentially driving more users and streaming activity to these networks.

Geolocation becomes complex in these environments where the consumer may be moving. Satellite networks are not limited to country borders and are often used in the marine and aviation industries to provide connectivity for travellers. Cellular networks are often used to provide connectivity on land-based transport services too.

To make IP-based geolocation even more challenging, these networks often deploy carrier-grade NAT (CG-NAT). This technology aggregates many consumer devices behind a single Internet IP address. This makes geolocation based on IP address impractical on these networks.

For services requiring country level geolocation, satellite connectivity may not provide reliable results. For services requiring state or city level geolocation, neither cellular nor satellite networks cannot provide a reliable geolocation.

International Cell Roaming

When users travel internationally, they may enable international roaming on their cellular device. When this happens, the user device's network traffic typically gets routed back to their home country where they are allocated an IP address. Network operators do this to allow for traffic management and billing.

For example, a UK user travelling to the US will have a UK IP address allocated to their device and will therefore be geolocated to the UK. As a result, IP-based geolocation is not reliable when cellular roaming, even for country level geolocation.

VPNs Widely Used And Hard To Detect

VPNs and other proxy services are in common use. With new legislation, such as the Online Safety Act in the UK and similar laws in other countries around the world, the demand for VPNs has spiked. An estimated 1.75 billion people are now using VPNs worldwide[2].

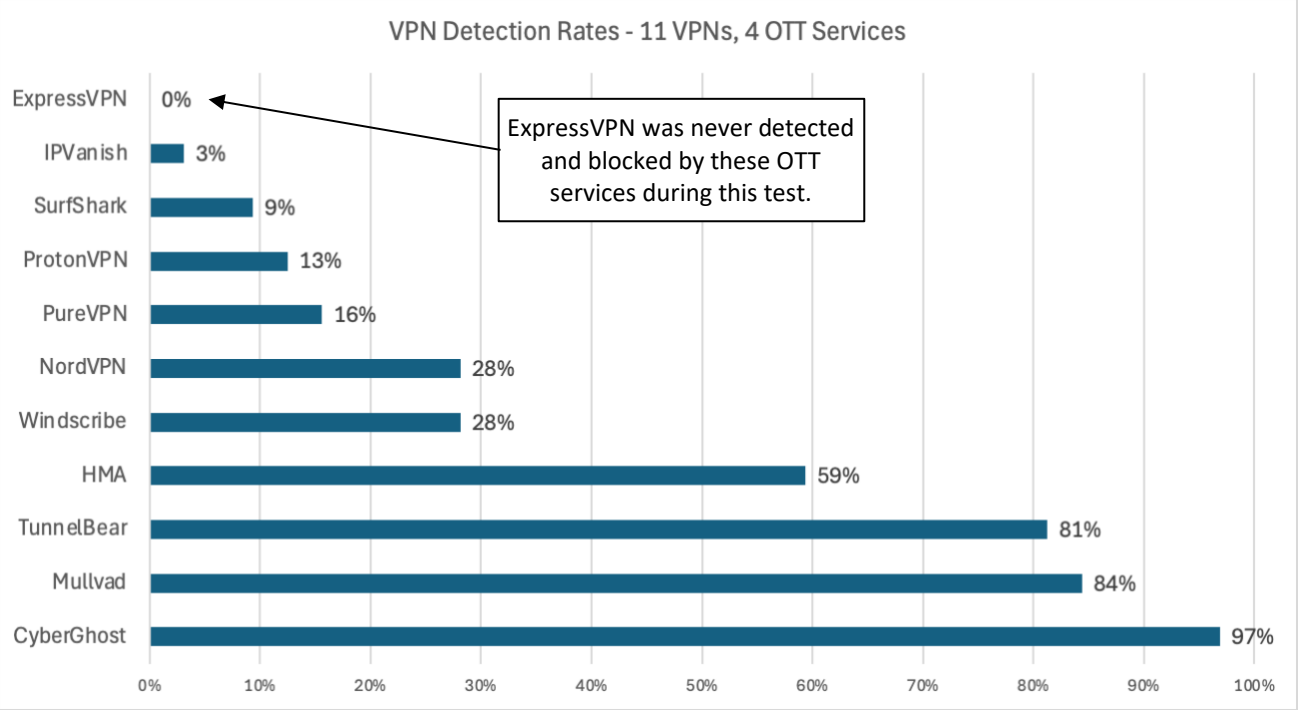
VPN detection vendors can detect VPN servers very accurately. However, VPNs deploy "Proxy over VPN" servers and residential proxies to evade detection[3]. When a streaming service is targeted with these technologies, detection rates fall quickly. Indeed, many VPNs can almost guarantee access to streaming services.

The following figure shows data from December 2025. Four major streaming services were accessed using 11 different VPNs.

[2] https://www.forbes.com/uk/advisor/business/vpn-statistics/#worldwide_vpn_usage_2025

[3] https://cdn.geocomply.com/wp/app/uploads/20230518141927/Residential-VPNs-A-Rising-Risk-for-OTT-Services-v1.0-GeoComply.pdf

Copyright © 2026 Kingsmead Security Ltd. All rights reserved.



We can see that VPNs targeting streaming services with proxy technology successfully avoid detection (e.g. ExpressVPN) and VPNs focussed mainly on privacy are detected and blocked more often (e.g. CyberGhost).

Detection rates can improve if a streaming service and their VPN detection vendor work together to detect and block proxy servers. However, successful proxy server blocking may simply encourage VPN vendors to deploy residential proxies. These proxies can take different forms, but essentially the VPN routes network traffic through an IP address that represents a residential home. A number of vendors now offer residential proxy services, which has driven down costs allowing more VPN vendors to deploy them. As a result, residential proxy usage is now commonplace amongst VPN vendors. Further, the widespread availability of residential proxies could allow pirate networks and more tech-savvy consumers to use these services directly.

Most consumers are unaware of residential proxies, and many may be unknowingly routing other people's network traffic through their own home. Some consumer devices and applications have embedded proxy server software pre-installed which enables this routing, potentially without the owner's knowledge or consent. This is a genuine cyber-security risk for those impacted.

Some VPN detection vendors detect residential proxy IP addresses, but streaming operators are unlikely to block them for fear of blocking genuine users. Using only IP addresses for geolocation does not give a streaming operator sufficient confidence to block these residential proxies and many operators simply accept that this activity happens.

We always recommend detecting and blocking VPNs to limit their impact and to provide some protection against cyber-security risks. However, streaming operators need to be aware that VPN blocking can have limited success.

Consumer Privacy Networks May Hide Location

VPNs are in regular use, but some major brands also offer their own Consumer Privacy Networks. For example, Cloudflare WARP or Apple iCloud Private Relay (IPR). IPR is a VPN-like service which aims to keep users' network traffic private. For most streaming services, only Safari network traffic uses IPR; other browsers and apps do not use IPR.

When configuring IPR, the user has two options regarding hiding their location:

- Assign an IP address which preserves general location

Copyright © 2026 Kingsmead Security Ltd. All rights reserved.

- Assign an IP address which preserves country and time zone

The first option is optimised for the consumption of local content; the second option is optimised for privacy.

Streaming operators can detect the use of these networks as VPN detection vendors will identify these IP addresses too. However, if the user has selected to hide their general location, their geolocation is not reliable enough for streaming services which require state or city level geolocation. This may prevent access to local content for some users and lead to customer dissatisfaction and support costs.

Risk Of Over-Blocking

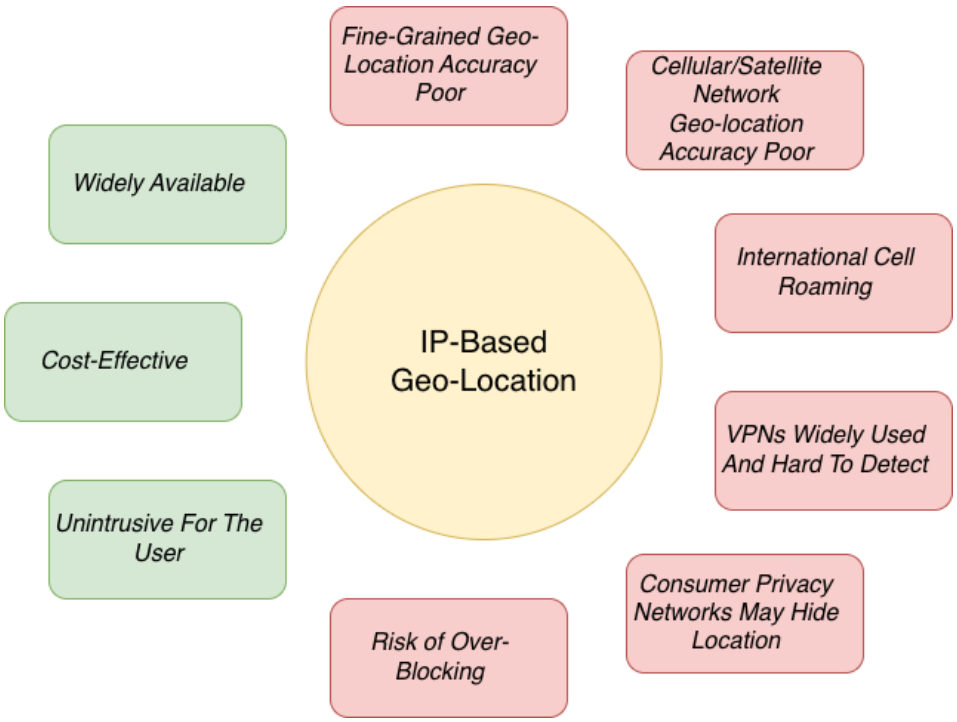
Blocking based on IP addresses can lead to denial of service for genuine users. For example, some locations such as hotels, hospitals, university residences, apartment blocks, etc. have Internet connectivity routed via data centres rather than a traditional ISP. This increases the risk of blocking which could lead to lost customers and revenue.

Summary

IP-based geolocation is simple, cost-effective, convenient and considered essential for all services.

However, IP-based geolocation can be inaccurate, especially on cellular and satellite networks. IP-based geolocation is not suitable for region or city level geolocation.

Further, VPNs have now reached a maturity level where they can reliably avoid detection. Where residential proxies are deployed to route VPN traffic, streaming operators have few options to defend themselves. VPN detection remains an important part of streaming service security, but a new approach may be required.



IP-based geolocation should always be deployed by streaming operators, but it should be used in conjunction with other forms of geolocation if VPN detection is poor or fine-grained geolocation is required. Further, as noted in Section 2, geolocation is not simply used to enforce content geo-restrictions but is an important tool to manage customer experience and malicious activity.

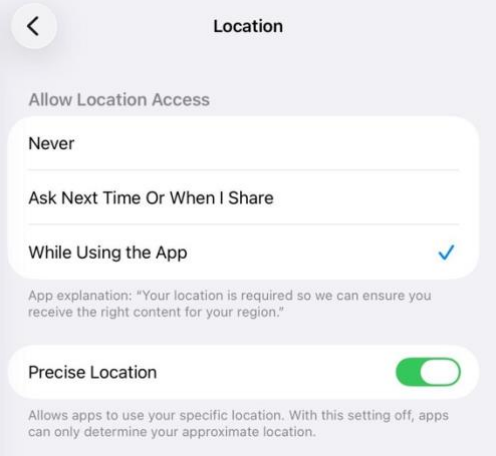
4 Beyond IP-Based Geolocation

Section 3 shows that there are limits to the accuracy of IP-based geolocation. To fully comply with contractual and legal obligations, and to provide a higher-quality customer experience, streaming operators should explore solutions beyond IP. Once deployed, these more sophisticated solutions enable new product and revenue opportunities for streaming operators.

Copyright © 2026 Kingsmead Security Ltd. All rights reserved.

4.1 Device-Based Location Services

Many modern consumer devices have built-in location services which a streaming service can use to confirm a user's location. Location services use a range of data sources to detect geolocation, including GPS, Wifi, cell towers, Bluetooth and IP address.



Advantages

Geolocation using location services is highly accurate, especially if based on sources such as GPS or Wi-Fi.

Once the user has granted permission to use their location, they are not prompted for permission on subsequent visits.

Disadvantages

Location Services Are Not Available On Some Devices

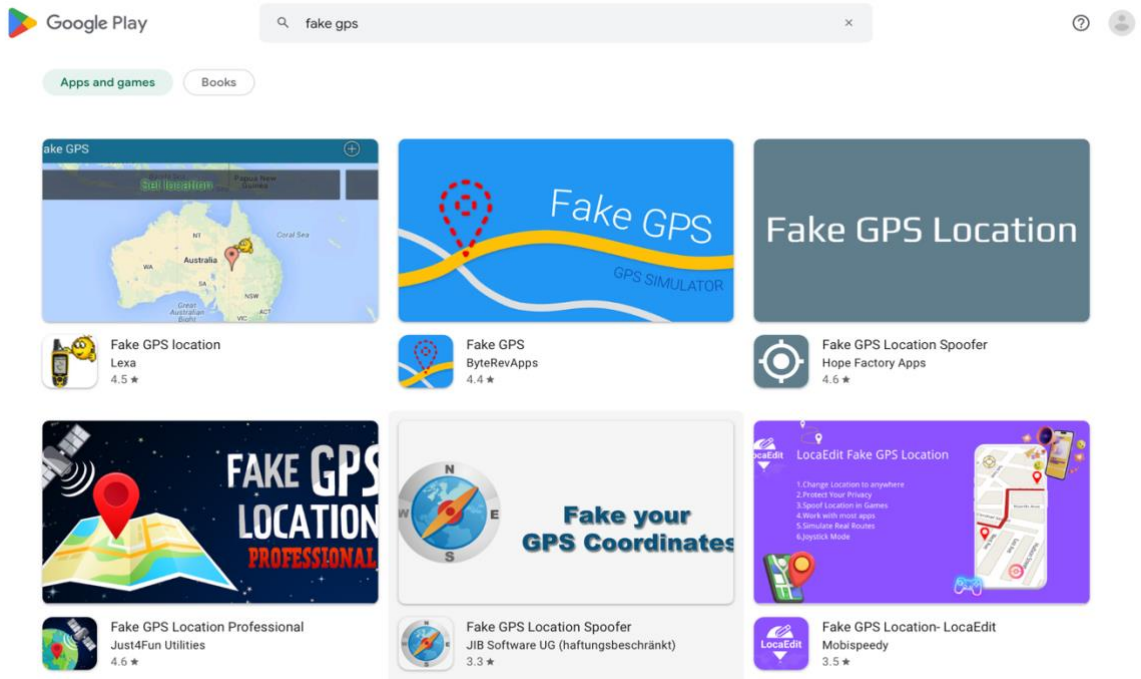
Cellphones are packed with sensors and can provide geolocation based on a variety of data sources. Other devices such as tablets and PCs may lack cell connectivity and GPS but can fallback to other sources such as Wifi or Bluetooth. Geolocation accuracy is generally good for these devices even when GPS is unavailable.

Devices such as Smart TVs have limited data sources suitable for geolocation and the application environment may not allow access to the data even if it is available. To obtain accurate geolocation information on these devices, services may use device pairing. It is already common to use a second device such as a cellphone to sign-in to Smart TVs as this avoids typing passwords. Streaming services could use this opportunity to obtain a location for the Smart TV from the pairing device.

Location Can Be Faked On Some Device Types

Some device types allow the user to fake locations. There are genuine use-cases for this feature such as testing a new application during development, but it can also be misused.

For example, many browsers allow the user to install browser extensions or use debuggers to fake a location. In addition, Android has many location faking apps, many of which have been downloaded millions of times. Examples of these apps are shown below:



Copyright © 2026 Kingsmead Security Ltd. All rights reserved.

Three of these apps have been downloaded more than 10 million times from the Play Store ("Fake GPS Location" more than 50 million times).

Some of these apps and extensions are tricky to use and would be inconvenient for a user to have enabled on every visit to the service. For example, Android fake location apps use Android developer features which must be enabled before locations can be faked. The poor experience may deter casual users from using them. However, some determined users can use these apps to fake their location.

Streaming services should check for fake locations (sometimes referred to as mock locations) and other application tampering when using location services.

Privacy Concerns For Some Users

Many users are concerned about privacy online. More disreputable websites can profit from user tracking, data sharing and data misuse. Many major brands such as Apple have used privacy to market their products and raise consumer awareness. These brands have also introduced services in recent years specifically targeted to protect privacy (e.g. Apple Private Relay and Apple Hide My Email).

Requesting location permission may deter some users and act as a barrier for others, leading to possible revenue loss. Worse, a user faced with privacy concerns and limited legitimate sources of content may be driven to pirate sources of content. This is a worst-case scenario for all parties.

Requesting location permission only when the user expects to be challenged and communicating the reasons why will help reduce privacy concerns. For example, the user may expect to be challenged when viewing an NFL game subject to blackouts but does not expect to be challenged when consuming a basic free-to-air news channel.

In preparation for possible future adoption, some streaming services are now including terms in their consumer contracts to allow for accurate location verification when viewing certain geo-restricted content. This is in addition to existing terms which prohibit geolocation circumvention, including using VPNs. Streaming services should plan to make these changes to future-proof their contracts as this helps to avoid surprises for the consumer.

4.2 Country of Residency Verification

Verifying the country of residency for a user is generally performed at sign-up. Streaming operators can perform this verification using methods such as:

- Payment method issuing country (with zipcode check).
- Local cellphone verification.
- Government issued verification methods (available in some countries only).

These methods do not give real-time geolocation information but can be used to verify residency.

Advantages

Geolocates Users, not Devices

Verifying the country of residence of a user is often a requirement in content licensing agreements.

Requiring a local payment mechanism is a major barrier to sign-up for unauthorised out-of-country users. Similarly, requiring a local cellphone to receive SMS passcodes can also act as a deterrent for out-of-country users.

Cellphone verification can also be used for two-factor authentication at login. This may be optional and only enforced if unusual patterns of activity are detected for an account (for example, logs in away from the home country).

For many contemporary services, payment method verification is an effective choice for residency verification.

Disadvantages

Copyright © 2026 Kingsmead Security Ltd. All rights reserved.

Local Cellphones Can Be Faked

Faking a local cellphone may be as simple as using the cell number for a genuine local resident and asking them to forward passcodes as they are received.

Alternatively, several online services provide disposable/temporary cellphone numbers in order to receive passcodes. Many of these are free to use. If a passcode is only required during sign-up, these services could be a simple and effective way to sign-up.

A determined user may also explore using eSims in their device. These could allow the receipt of SMS messages out-of-country, although many eSims are restricted in some way (e.g. no international roaming, data only).

Expat Communities Impacted

For some countries with large expat communities such as the UAE, payment method or cellphone verification can block access for users still relying on cellular and banking services from their home country.

In these countries, residency verification may not be possible, so accurate geolocation technology is required.

Adds Friction During Sign-Up

Streaming operators seek to ensure that their sign-up process is as streamlined as possible. Each new step during the sign-up process adds friction which has the potential to deter sign-up. Although lost sign-ups may be rare, a lost sign-up is lost revenue.

The reality is that streaming operators often prioritise friction reduction over other concerns. Acquisition and retention of their subscriber base is their raison d'être.

Replacing payment method or cellphone country of residence verification with accurate device-based geolocation detection could streamline the sign-up process, reducing the barriers to entry. This reduces the risk that disgruntled users may be attracted to pirate sources of content – a worst-case scenario for the industry.

4.3 Other Methods of Geolocation

Other sources of data are available which may help detect location and location faking.

For example, if the timezone configuration of the device does not match the timezone of the service operating country, then some suspect activity may be in progress. Other device settings such as language can also be used.

These settings can easily be changed by a user and therefore only provide very weak evidence of location. However, if used in combination with other forms of geolocation, they can provide further evidence or indicate potential faking.

Some vendors combine IP geolocation, device-based location services and these other methods of geolocation together to deliver a very robust geolocation solution.

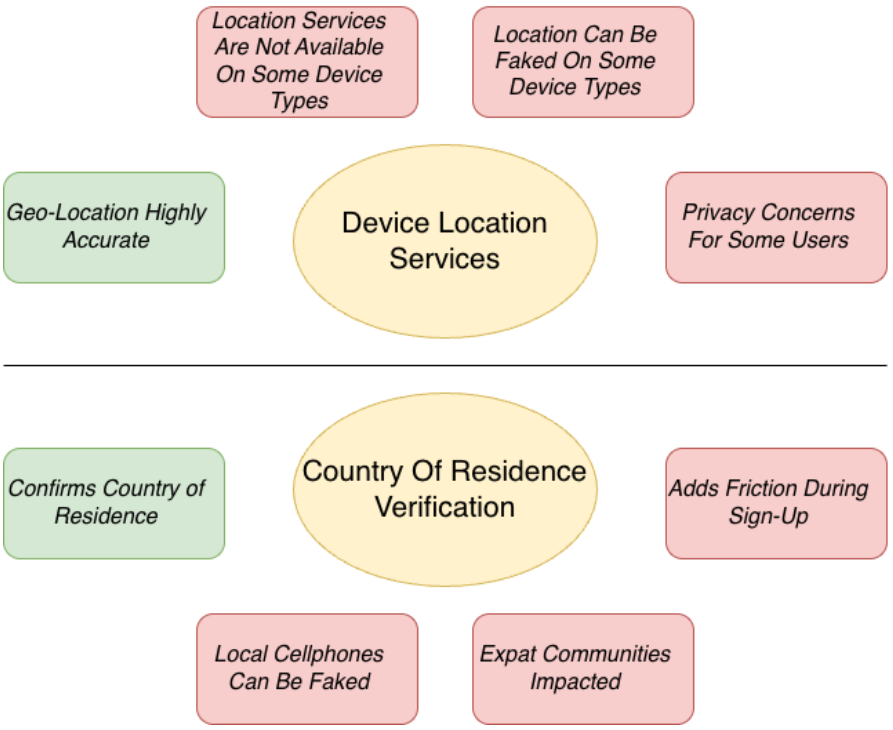
Copyright © 2026 Kingsmead Security Ltd. All rights reserved.

4.4 Summary

Device-based location services provide a very accurate geolocation solution for use in streaming services. The accuracy allows for the creation of very localised products and services.

On some devices, location can be faked using apps and extensions. A number of users may use these tools, but many will be deterred by their technical nature. For streaming operations, the impact of these tools can be minimised by detecting their presence.

Privacy is a concern for many users, who may suspect unwanted tracking activity when asked to provide their location. We recommend streaming services avoid surprises and communicate clearly to the user to manage these concerns.



Residency verification aims to ensure that only residents of service operating countries can sign-up. Payment method or SMS verification are common options for verification.

5 Current Usage

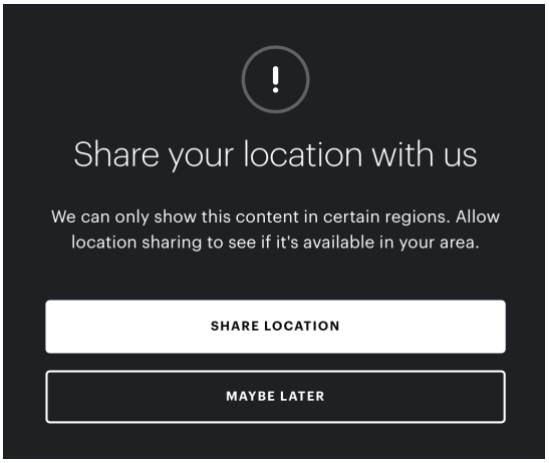
IP addresses are the standard method for geolocation and are widely deployed by most streaming services. Services not deploying IP-based geolocation risk breaching licensing contracts and are exposing themselves to a higher cyber-security and fraud risk. Geolocation beyond IP is in place for some services, although usage remains rare.

Android and Apple have two levels of location services:

- “Precise location” is potentially accurate to a few feet and uses GPS.
- “Approximate location” or “Coarse location” is accurate to a few square miles and does not use GPS.

Using data safety information shown on the Google Play Store and Apple App Store, we can find a selection of streaming services confirming use of precise location services:

- 7Plus
- ESPN
- Foxtel
- Hulu
- Prime Video
- Sling
- YouTube TV



Copyright © 2026 Kingsmead Security Ltd. All rights reserved.

This is not intended to be an exhaustive list. However, we can see that precise location is used by a growing number of apps. These are predominantly using location services to meet the needs of sports content licensing deals. Some may also have other specific requirements for more accurate location.

These apps generally only ask the user to provide location permission when it is required. If the use of location services is limited to only specific content items or app functionality, then the user may never be prompted to agree.

Where more sophisticated geolocation technologies are used, it is important to ensure that users cannot mock their location using tools such as apps or browser extensions. Hardening the client application against tampering and using multiple sources of location information will protect against unauthorised use.

6 Future Outlook

As the streaming industry continues to grow and evolve, along with the network technologies which underpin it, we are likely to see greater use of sophisticated geolocation technologies.

For **rights owners**, current levels of compliance to geo-restriction requirements can be low even for streaming operators meeting recommended best practice due to the widespread use of VPNs and other location masking technologies. More sophisticated geolocation solutions can improve compliance and potentially unlock new licensing opportunities. Local content rights, sports in particular, could be enabled by more accurate geolocation.

For **streaming operators**, more sophisticated geolocation solutions ensure better compliance to licensing obligations. Further, accurate geolocation could improve detection of fraudulent or malicious activity, reduce lost revenue and assist in the fight against piracy. Accurate geolocation could also enable new revenue opportunities such as family sharing and second home subscriptions.

For **advertisers**, the ability to target end users based on accurate location is very valuable, creating new opportunities for targeting and enabling new markets in local business advertising.

For **consumers**, more sophisticated geolocation solutions could streamline signup processes by removing the requirement for local payment options or local cellphones. Recommendation engines could also be optimised to deliver content recommendations more suitable for their local area.

For **regulators**, more sophisticated geolocation solutions ensures that streaming operators have the technologies required to meet local regulations. We have already witnessed the widespread use of VPNs to avoid local regulations. Examples include the UK's Online Safety Act which requires age verification to consume adult content[4] and Australia's Online Safety Amendment (Social Media Minimum Age) Act[5] which bans social media for the under-16s[6]. Widespread VPN use, combined with current VPN detection technologies, has driven many VPN vendors to utilise residential proxy networks to avoid detection. These proxies represent a very serious cyber-security risk to the public within their own homes.

[4] https://www.bbc.co.uk/news/articles/cvg5er4ewg6o

[5] https://www.legislation.gov.au/C2024A00127/asmade/text

[6] https://www.theguardian.com/australia-news/2026/mar/09/vpn-downloads-australia-porn-sites-blocking-users

Copyright © 2026 Kingsmead Security Ltd. All rights reserved.

Kingsmead Security Ltd

Web: www.kingsmeadsecurity.com

Email: contact@kingsmeadsecurity.com

Conclusion

Geolocation is required for streaming services to meet their business, contractual and legal requirements. IP-based geolocation is the standard method used throughout the streaming industry and is essential for all streaming services. However, as the industry evolves, new products and services will require a level of geolocation accuracy that IP-based geolocation cannot deliver.

There are many reasons why IP-based geolocation fails, including increasing cellular/satellite connectivity and VPN use. Performance of IP-based geolocation quickly degrades when fine-grained geolocation is required to manage content licensing requirements such as sports blackouts.

All streaming operators should deploy IP-based geolocation as a minimum, but more accurate methods are increasingly required and are being deployed by a growing number of operators. Device-based location services are the obvious additional control, but this should be deployed in conjunction with measures to increase robustness and prevent tampering.

Effectively deployed, these more sophisticated geolocation solutions enable a better customer experience, create new product opportunities, and unlock new revenue streams for rights owners and streaming operators. However, these solutions should be deployed whilst bearing in mind consumer concerns regarding privacy and location tracking.

We forecast increasing use of geolocation solutions beyond IP in the coming years and look forward to observing the industry innovations these solutions unlock.

For independent advice on protecting your OTT service, please contact Kingsmead Security at contact@kingsmeadsecurity.com or visit www.kingsmeadsecurity.com.

Copyright © 2026 Kingsmead Security Ltd. All rights reserved.