GEOLOCATION: Solutions to Common Issues & Misconceptions

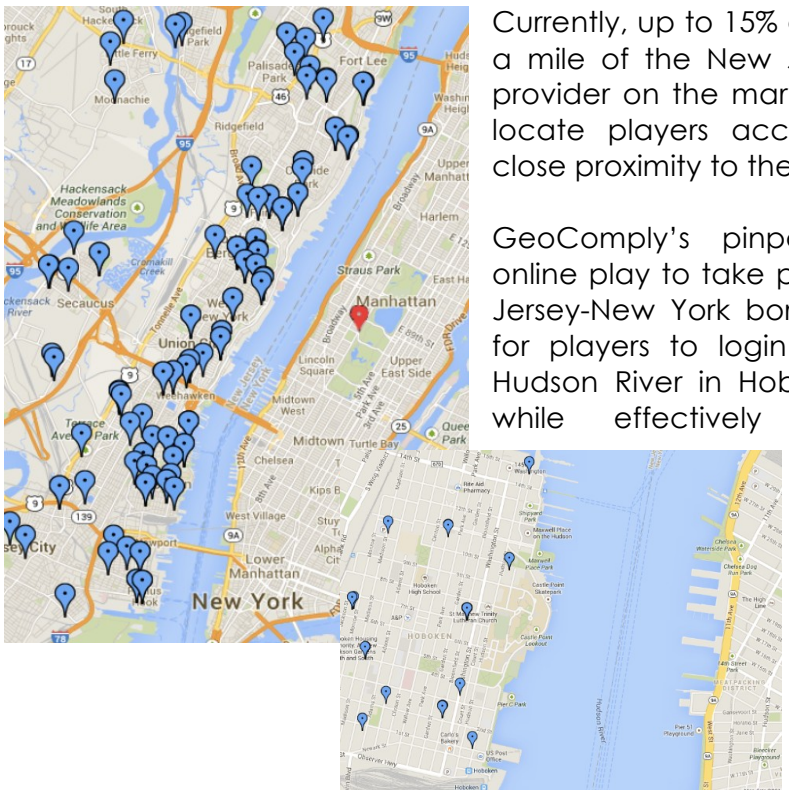
Key Aspects of our Proprietary and Patented Geolocation Solution

GeoComply is able to deliver such precision due to its patented technology solution, which analyzes and encrypts multiple data sources from a user's device. **GeoComply collects IP, Wifi, GSM, GPS and Carrier location data**. No other location solution exists on the market that provides this level of cross referencing to best determine user location to satisfy compliance needs and anti-fraud systems.

GeoComply's uniquely tailored approach increases its accuracy and reliability. Reliance upon multiple data sources, layered with comprehensive fraud-checks, sets GeoComply apart from previous solutions which typically rely solely upon one data source. Due to the inherent difficulty of accurate geolocation on the internet for regulated industries, sole reliance upon one data source presents an increased risk of inaccurate or imprecise results.

LEADING THE NJ MARKET

As the geolocation provider to 100% of New Jersey brands, GeoComply proudly dominates the New Jersey market with unrivalled geolocation solutions to assist operators comply with the world's most stringent geolocation regulations. We do so with remarkable precision and ease of use.



Currently, up to 15% of play takes place within a mile of the New Jersey border. No other provider on the market is able to successfully locate players accurately enough in such close proximity to the border.

GeoComply's pinpoint accuracy enables online play to take place right up to the New Jersey-New York border. Our solution allows for players to login from the banks of the Hudson River in Hoboken or Jersey City, NJ, while effectively blocking play from neighboring Manhattan just across the River in New York.

GEOLOCATION: Solutions to Common Issues & Misconceptions

RECORD BREAKING SUCCESS RATES

US iGaming operators have come to rely on GeoComply for the assurance that they will be compliant with all applicable laws and regulations concerning geolocation.

Having consistently increased our success rate since the New Jersey launch in 2013, operators across the U.S. now have 98% or more of their players passing geolocation checks.

These numbers far exceed the performance of any other geolocation service provider – all while being subjected to the world's most stringent geolocation standards. We continue our efforts to increase the success rate even higher as we strive to help operators maximize player acceptance while retaining cost per acquisition costs.

UNPARALLELED ANALYTICS & FRAUD PROTECTION

Providing a service beyond the simple processing of transactions has been the driving force behind GeoComply's record-high pass rates. Built on the foundation of our robust back office system, the power of GeoComply's solution is in the richness of the data it gathers.

GeoComply's back office system allows for in-depth analysis and logging of all transactions that take place. Automated reports can be scheduled at regular intervals while custom reporting allows for detailed analysis to gain greater insight as the needs arise.

GeoComply's advanced technologies offer an invaluable way for operators to stop collusion, as well as for payment gateways and merchants to prevent fraud and improve chargeback rates. Working closely with the payment providers, GeoComply has been able to reduce the cost of chargebacks to their merchants by at least 85%, simply by leveraging their powerful data collection tools.

> "GeoComply were able to cut our payment fraud costs by at least 85%. Their solution gave us access to more detail and data than we had ever had before for our eCommerce transactions. Their anti-fraud reports were literally good enough to take to the bank in order to win our charge back disputes!"
> - Omer Sattar, Senior VP, Sightline Payments

GEOLOCATION: Solutions to Common Issues & Misconceptions

Location Code of Conduct- Respect States' Rights

- Geolocation solutions used must always be accurate enough to locate player as **definitely within the permitted State's Borders**
  - **"Bleeding" across borders** will not be tolerated so the highest accuracy methods of geolocation are preferred (WiFi and/or GPS, rather than Cell Tower triangulation and/or GSM),
  - if data Accuracy Radius returned is not accurate enough and/or it overlaps with a bordering State the end user will be blocked
  - Boundary definitions (geographic coordinates) should be obtained from a state or Federal Government database.
- Any solution used can not be **"self-certified"** but must be independently verified, via Field Tests, as meeting standards required by UIGEA/DOJ requirement for sufficient geolocation tools;
  - Independent verification should be from a body such as a state approved testing facility or government testing facility.
  - Independent Verification must include field trials with common location spoofing methods (inc. those listed in this document)
- IP Geolocation is not acceptable as the sole location data source (as it has the highest risk of vulnerability) without significant additional checks
  - IP location data cannot be considered for mobile (3G) transactions as it represents the location of the carrier and not end user device.
  - Additional verification must be more than just a database of known Proxy's (as these are so incomplete). Multiple measures such as DNS Proxy Detection, Proxy Piercing, Algorithmic Analysis for Probability of Fraud etc would ALL have to be used to accept IP from Static ISP's as a usable form of Geolocation data.
- Use of an end user's "billing address", residence, or KYC history in an allowed territory is not an acceptable method of geolocation.
- For native applications. the geolocation solution used must be able to analyze the programs running on the device to detect location spoofing applications, and recognize whether the device has been compromised, e.g. a rooted or jail-broken smart phone.
  - "VPN Protection" shall be used; VPNs and other methods of location spoofing such as Proxies, DNS Proxies, Remote Desktop Programs, etc must be detected and blocked.
- Mobile/3G connected players (including players on a Laptop with a 3G USB dongle on a train for example) must be recognized as being on a mobile connection (not a Static Landline connection). Their re-location frequency must be established in proportion to their proximity to the nearest border & the earliest time their session could breach the border.
- Data analytics must be carried out to recognize players attempting to spoof location.
- Best practice security measures should be in place to ensure "man in the middle attacks" to emulate a successful geolocation result
  - Including encryption standards, license authentication and effective data analytics to detect any such attack