



ISO 27566-1 Practice Statement

Solution Owner: GeoComply

GeoComply is a(n) Intermediary (entity that facilitates the interaction between individuals, age assurance providers, relying parties, and other parties to fulfil functions in an age assurance system)

This is a practice statement for the age assurance solution known as GeoComply Core

The system and practice statement are kept under continuous and regular review in the following way:

GeoComply is a supporting technology for age assurance processes and is not an age assurance provider, relying party, nor intermediary. Therefore, we do not strictly adhere to ISO 27566-1 and do not currently maintain a formal practice statement.

However, we do have functionality, performance, information security, cybersecurity, and privacy protection documentation, practices, and processes that are maintained by the appropriate teams within GeoComply, in accordance with our regulatory obligations.

The role and impact of the intermediary is as follows:

GeoComply conducts extensive data analysis to determine whether a user seeks to access an online platform from a jurisdiction in which said platform has specific compliance obligations, including age verification. GeoComply can determine the location of a platform's end user, regardless of whether the user employs technology to obfuscate their digital location signatures.

GeoComply integrates directly with specific online platforms. Our system uses a vast and regularly updated Internet Protocol (IP) address database to determine if an IP address, ostensibly associated with a specific device and location, is in reality associated with a location-obfuscating tool, specifically a virtual private network (VPN) or the Onion Router (Tor). Additionally, with user permission, GeoComply conducts GPS, Wi-Fi, and cell tower signal triangulation to determine the precise latitude and longitude of a device. GeoComply aggregates all of this information, along with additional data points, to determine whether the user's online experience is subject to specific laws and associated technical compliance processes. We then send a response to the online platform with a determination as to whether additional processes (in this case, age assurance processes) need to be applied.

As stated above, while GeoComply is not an covered age assurance technology, and therefore does not strictly incorporate ISO 27566-1 standards into our processes, functionality, performance, privacy, and security, are all critical components of our processes, products, and technology.

Regarding functionality: GeoComply ensures our systems remain maximally effective by maintaining negligible rates of false negatives (the number of users inaccurately located, despite untampered location data) and false positives (the number of users who bypass our location spoofing detection to falsely appear within a specific area). While there is no single minimum efficacy requirement, with different geolocation use cases and regulatory environments all having unique standards, GeoComply easily clears such minimum standards of effectiveness in all operating environments. This will be further explained under "Audit, Certification, and Review".

Regarding performance: GeoComply's systems are designed to scale with increasing customer demand for our services. We regularly process over 1 billion geolocation transactions per month and in cases where an organization

may have a high volume event, GeoComply has the ability to scale its system's environments to account for the spike in traffic. GeoComply has maintained an uptime in line with and exceeding industry standards.

Regarding Security: Our Information Security Program (ISP) includes various technical and organizational security measures to protect our product environments and company systems, such as access controls, personnel training, physical security, network and cloud security, credential and key management, and software development lifecycle policies and practices. Specifically, GeoComply uses TLS 1.2+ encryption protocol for data in transit and at least AES 128 data encryption protocol for data at rest.

Our Information Security Program (ISP) is regularly audited by a third-party auditor as part of a SOC 2 audit, and we maintain SOC 2 certification as a result of these audits. SOC 2 is a report that evaluates an organization's information systems with regard to security, availability, processing integrity, confidentiality, and privacy, based on the Auditing Standards Board of the American Institute of Certified Public Accountants' (AICPA) Trust Services Criteria (TSC). We can provide our customers with the most recent SOC 2 report upon request and under a non-disclosure agreement via our Security Portal.

Regarding Privacy: We only collect the data necessary to verify a device user's location to the requisite regulatory/fraud detection standard. This varies by circumstances. GeoComply's passive tools will collect a device's IP address. With an end user's consent, GeoComply will collect GPS satellite data, wireless and cellular network data, and internet connections. GeoComply may also collect other device information to determine if a user is attempting to mask their location. Device performance, network performance, memory usage, and clock differences reported by different means can be used to understand whether a user is really where they claim to be.

The location data in our possession was provided to us for a specific purpose determined by our customers, primarily anti-fraud and compliance use cases; we do not resell or cross-share this personal information with other customers, nor do we use any data that may directly target individuals or customers for other purposes.

GeoComply has developed an existing robust privacy framework to work with its customers to ensure personal information is processed and managed in accordance with applicable data protection laws, including the GDPR, PIPEDA, CPRA, and COPPA. GeoComply's Data Processing Addendum, created with the GDPR, PIPEDA, CPRA, and COPPA in mind, is designed to facilitate this processing and management. This existing privacy framework should be materially sufficient to comply with the Australian Privacy Act and Children's Privacy Guidelines.

GeoComply pseudonymizes our data. We associate device-level data with a user ID of a customer's choosing. As a result, we do not have an end user's name, email address, etc. Our customer is responsible for joining our device-level data with their data that contains the identity of the end user.

The following age assurance providers and relying parties are supported:

GeoComply can support relying parties with age assurance obligations, including gaming, media and entertainment, and social media companies. We currently support companies in these industries with determining end user location for compliance purposes, including but not limited to age assurance.

As GeoComply's technical geolocation services are functionally unique from the age assurance process, we do not directly overlap with the activities covered by relying parties' practice statements.

The solution has been subject to audit, certification and review in the following ways:

GeoComply operates in a number of unique regulatory environments in which we must comply with prescriptive geolocation regulations. In accordance with these regulations, our technology is tested by the relevant authorities. GeoComply maintains approximately 60 licenses, primarily issued by subnational entities (i.e., U.S. states, sovereign tribes) that reflect our ability to meet the minimum regulatory standards within a specific jurisdiction. A list of these licenses, and the corresponding regulatory standards, may be made available upon request.

Primary Contact Details

Lead Contact

[REDACTED]

Lead Contact Email

[REDACTED]

Lead Contact Phone (with country code)

[REDACTED]