SOVEREIGN INTELLIGENCE

Make sense of the world's data so people can make better decisions.

Aurora:GeoCanvass®

Global Geolocation Intelligence Software

AURORA:GeoCanvass® helps law enforcement and national security agencies generate leads quickly. The Aurora: GeoCanvass® leverages proprietary data analytics to discover the presence of device activity for an Area and Time of Interest.

Built on the Aurora:GeoStudio® platform, the Aurora:GeoCanvass® helps you discover the geolocation of smartphone devices on a global scale. Our theory is that if you can observe *where* people go, you can learn *why* they are there. Aurora:GeoStudio® is designed to bring an enhanced level of confidence surrounding the discovery of answers for two reasons: (1) our proprietary ability to know where to look among the vast libraries of geolocation data, and (2) our advanced data analytics to help you observe otherwise indecipherable data patterns for better insight. Welcome to Sovereign Intelligence.

AURORA:GeoStudio® survey's over 600 million smartphone devices on a global basis every day. No other software platform in the industry accesses this much data across the world, while delivering a user-friendly interactive studio experience, fit precisely for analyst's.

Aurora: Location Intelligence-as-a-Service

Aurora:GeoCanvass® solves the industry's most significant problems with discovering location intelligence insight.

Lead Generation
Aurora:GeoCanvass® provides law enforcement with leads derived from mobile device activity related to an area and time of interest.

Lead Prioritization
Aurora:GeoCanvass® prioritizes lead generation for law enforcement by delivering device details, including the best time and location to follow-up on the lead.

Target Generation
Aurora:GeoCanvass® provides national security agencies with leads derived from mobile device activity related to an area and time of interest. Receive enhanced targeting details regarding device activity.

Target Prioritization
Aurora:GeoCanvass® prioritizes lead generation for national security agencies by delivering device details, including the best time and location to engage the target.

Data Questions

Data	Answers
What is geolocation metadata?	Geolocation metadata includes information derived from geo coordinates of an activity (addresses, points of interest, etc.) or devices along with date and time of the information. Metadata enrichment can add other information depending on the richness of metadata (i.e., network address, provider, etc.).
Where does this data come from?	Data is provided from various applications on smart devices that use what is known as a Mobile Advertiser Identifier (MAID). From those applications, the data is compiled, cleaned, and analyzed for accuracy and deduplication before it is passed on to the Aurora application.
When does geolocation data become available?	Geolocation becomes available as soon as it is received from the application provider. Generally, 25%-50% of the mobile devices are identified within 24 hours, 75% within 2 days and 100% within 3-4 days of the current date.
Can you identify the device IMEI?	No. That information would only be available from mobile carriers or Internet Service Providers.
Can you identify the application used?	No. The data is collected by applications that utilize specific SDKs (software development kits), but is not included in the data feeds.
What does the 2-word device name represent?	This is an internal naming system for reference only. Commonalities between device names does not indicate a relationship of any kind between the devices.
What is What3Words?	"What3Words" is a universally accepted way to describe a precise location anywhere in the world. The terminology divides the world into 3m squares and gives each one a unique identifier made from three random words. Similar to GPS coordinates, we use What3Words to provide Law Enforcement with an easy to reference location of a new lead. To learn more about What3Words, visit: https://what3words.com/about
How accurate is the location?	The geolocation data is accurate within a few meters and is based on how the application tracks the information. For example, a home wifi signal might be accessible 20 meters from the source so a mobile device may show outside the home, not the center of the signal.
Why are there no devices in a search area?	There are a variety of reasons why you may not see a device you expect to see in an area: 1. The device user has turned off their Location Services. 2. The device user is not using applications that are included in our data collection. 3. The device doesn't have a geolocation receiver or other means of determining its location. 4. The device's geolocation receiver is not functioning properly. 5. The device's location services are turned off or restricted. 6. The device is in an area where it is difficult to obtain a geolocation report from the device. 7. There is interference with the geolocation signal, such as from tall buildings or other objects that block the report. 8. The device is being used in an environment where the geolocation is unreliable, such as in a tunnel or under heavy tree cover. 9. The device's MAID is not properly configured or is experiencing an issue that prevents it from reporting location information.

Application Questions

Application	Answers
Why is the radius of the search 100m?	Geo100m is a reasonable distance from which witnesses could view an event. Also, there is a chance that a device of interest may have sent a geolocation report before entering or after leaving a location of interest. Multiple searches may be performed to capture data in more than one location.
Why is the time period set to 30 days before and after the queried event?	It's 30 days in both directions currently to pick up on possible important behaviors that happened before or after the incident.
How far back can I query?	The event date may be set up to two years back from today's date. For example: If you're interested in an event dated May 5, 2022, that date can be entered. Then, the +/- 30 days from that date would be applied.
Can I get a location history for a specific device?	Location history for specific devices is not currently available, but may be part of a future release. See Aurora: GeoStudio® to access historical views.
How does the ranking system work?	The ranking system is based on weighing multiple factors involving the frequency and density of device activity relative to the time and location of the event. A device that is both closer in time and space to the event time is ranked higher than those that aren't. However, if the frequency of a device is particularly high it may be ranked higher because it has been assessed by our A.I.to be extremely important to lead generation. For example, an armed robbery occurs at a bank across the street from a coffee shop at 1pm and a device has been identified that frequents the shop everyday from 10am to 2pm. This device may not seem as relevant in time and location as a dog walker that walked past the bank at 12:55 pm, but will be ranked higher given the likelihood of the coffee shop patron to provide a more important lead. Based on their observations of what is considered routine, they may have seen something out of the ordinary.

Legal Questions

Legal	Answers
Is there legal precedent for law enforcement to use this data?	Many local and federal law enforcement agencies already use this data to generate leads.
How does Law Enforcement use this kind of data?	Law Enforcement strictly uses the findings as a “lead generation tool.” This means that actual evidence collected to determine the location of a suspect in a crime, must be derived from an approved warrant in accordance with *Carpenter, et al*. In *Carpenter v. United States*, the U.S. Supreme Court in 2018, held that a warrant is required for police to access cell site location information (CSLI) from a cell phone company—the detailed geolocation information generated by a cellphone’s communication with cell towers. Warrantless access to CSLI is still allowed in exigent circumstances.
Can I use this output as evidence?	This is a lead generation tool and is not sufficient for evidence purposes. Think of it like a flashlight. It helps you see what is in plain sight, but the “flashlight” isn't entered into evidence. The geolocation metadata that applications have generated is a reflection of the movement of a smartphone. According to *Carpenter, et al*, a subpoena is required to access relevant telecommunications data which is the authenticated information a smartphone needs for evidentiary purposes.
How do attorneys in court prove the data is anonymous?	The system doesn't provide any data that would be used in court. The only data that is used in court comes from the telecommunications companies and Internet Service Providers after they have been subpoenaed. The system delivers a ranked list of devices discovered in the search and specific times for the ISPs and mobile carriers to quickly turn around information requests. We are providing lead generation insight which tells an officer, "Hey, there were devices of interest here (time and place). Now go back to these locations and talk to folks who may know something about the crime."
What mechanism do the app providers use to both confirm consent and that they have the right to share the anonymized information?	We access open source data based on direct consent through the "opt-in" behavior each smart device user exercises when downloading and turning on location services for an app. Location Services are governed by the smart device user.

Enterprise Solutions Suite

Aurora:CIMS®

Sovereign has developed the most disruptive intelligence software the world has ever seen. AURORA solves the problem of weak decision-making, whether instigated by siloed data, inadequate intelligence collection, biased AI assumptions, or stymied sense-making capacity.

Aurora:GeoStudio®

Aurora:GeoStudio® helps you discover the geolocation of smartphone devices on a global scale. Our theory is that if you can observe *where* people go, you can learn *why* they are there. We observe over 16 billion geolocation events and over 600 million devices every day.

Aurora:AddScore®

Aurora:AddScore® helps financial institutions verify the addresses provided by a loan applicant. To avoid fraud, and to prevent money laundering, bank's need a fast, secure, and discrete method to confirm an applicant's home or work address. The Aurora: AddScore® leverages our Aurora: GeoStudio® data analytics to quickly confirm the presence of devices during a history look-back at the applicant's activity.

Aurora:GeoCanvass®

Aurora:GeoCanvass® provides commercial or government entities automated geolocation attribution of devices discovered during Area of Interest for sensitive site locations, retail marketing/advertising, as well as national security related intelligence collection

Aurora:NetIntel®

Aurora:NetIntel® provides a singular focus not only on in-network vulnerabilities and associated risk ratings but also expands and connects into the Threat Actor Landscape revealing the potential for stolen or exposed Intellectual Property, Code, and PII. Built for IT Security Professionals.

Service Offerings	Aurora:CIMS®	Aurora:GeoStudio®	Aurora:AddScore®	Aurora:NetIntel®	Aurora:GeoCanvass®
Type	Enterprise	Enterprise	Enterprise	Enterprise	Enterprise
Optimal Clientele	National Security/Corporations	National Security/Corporations	Financial Institutions	Corporations	Law Enforcement/National Security
Delivery	1 API	1 SaaS	1 API	1 API	1 API
Term	1 Year	1 Year	1 Year	1 Year	1 Year
Pricing	Based on Scope/Usage	License Fee Based on Usage	License Fee Plus Pay-per-search	License Fee Based on Usage	Based on Scope/Usage
Payment	Yearly Upfront	Yearly Upfront	Yearly Upfront	Yearly Upfront	Yearly Upfront
Return	Full Software Interaction	Full Software Interaction	Metrics/Report	Metrics/Report	Geolocation Attribution Report