Geolocation and Application Delivery

The data from geolocation providers offers highly valuable data to a variety of stakeholders and is no longer just for advertising.

by Lori MacVittie
Technical Marketing Manager, Application Services
## Contents

**Introduction** 3

**Geolocation Use Cases** 3
- Enforcing Location-Based Restrictions 4
- Optimal Request Routing and Cloud Balancing 5
- Context-Aware Security 5
- Enhanced Visibility 6

**Geolocation Implementation** 7

**Conclusion** 8
Introduction

In the past, the use of geolocation technology was limited to content delivery networks (CDNs) and targeted advertising. In both cases it was necessary to determine the client’s location with as much accuracy as possible in order to intelligently route application requests to the nearest data center for optimal user performance or to more effectively deliver relevant advertising.

As the accuracy of geolocation technology has improved, there are more use cases for location-based networking than ever before. Advertising and performance-related implementations are still valid use cases, but the enforcement of location-based access restrictions and context-aware security is quickly becoming more important, especially among an increasingly mobile user base.

Also of rising importance is cloud computing, which introduces new challenges to IT in terms of global load balancing configurations. Hybrid architectures that attempt to seamlessly use public and private cloud implementations for scalability, disaster recovery, and availability purposes can leverage accurate geolocation data to enable a broader spectrum of functionality and options.

Geolocation Use Cases

When geolocation data is highly accurate, it can be employed across a broader set of functions that might depend on or be enhanced by having access to that information.

The key is to ensure the geolocation technology is, in fact, as accurate as possible. This often requires that a solution wishing to take advantage of geolocation capabilities must look to an outside source. The traditional methods of geolocation have depended upon public IP address registries, which are now highly suspect in regard to accuracy and thus cannot be depended upon to provide valid location information. Using a trusted third-party source for location determination enables solutions to apply location-based policies with a high degree of assurance that the data is accurate. This level of accuracy permits a broader set of uses for geolocation technology.
Enforcing Location-Based Restrictions

Many IT professionals might recall that in the early days of SSL implementations, technology enabling 128-bit key certificates could not be exported outside the United States. This restriction applied to digital content, such as browsers, too. The restrictions were extremely difficult to enforce at the time because geolocation technology was in its infancy and highly inaccurate.

Today, the U.S. continues to impose similar restrictions on technology offerings, especially those involving security and cryptography. The enforcement of such restrictions has become easier as geolocation offerings have matured.

It is not just legal-based regulatory restrictions that need enforcement, however. The increasing broadcast of video-based content and live events has given rise to concerns regarding how to enforce broadcasting restrictions, as well.

For example, a Norwegian broadcaster may have rights to stream the Olympics in Norway, but needs to block access to users coming from other countries because it only has rights to broadcast in Norway. And, within the U.S., the National Football League has specific requirements that may prohibit the live broadcasting of football games in specific areas based on whether the game is sold out. In these and other instances, solutions that have the ability to determine location with a high degree of specificity—for example, by postal code—will prohibit or permit access to broadcasts.

Figure 1: U.S. trade restrictions require blocking access to certain locations.
A highly accurate geolocation implementation provides the necessary level of granularity, and ensures that trade, broadcast, and other location-based restrictions can more easily be enforced.

Optimal Request Routing and Cloud Balancing

Geolocation data provides more information than its name implies. Included in highly accurate geolocation data can be information germane to making application-request routing decisions.

The use of geolocation for proximity-based access to applications transparently benefits all users. Users directed to the application instance or website that is physically closest to them mitigates the impact of speed of light limitations on application performance. For organizations with very large web presences, basing decisions on physical proximity is also an efficient method of distributing resources. The integration of accurate geolocation technology helps organizations scale applications appropriately—providing, for example, more compute resources in New York, where there are millions of users, and fewer resources in Topeka, Kansas, where there might be only a few thousand users.

Cloud balancing is the routing of application requests across applications or workloads that reside in multiple clouds. It assumes that all instances of the application deployed in the various clouds are accessible at all times. A large part of the value proposition of cloud balancing is to optimize resource utilization while simultaneously enhancing user performance. Geolocation data advances this process by supplying information about the user connection that can be valuable to a global server load balancing solution that is attempting to find the optimal data center or cloud to which that user’s request should be directed.

Context-Aware Security

The increasingly mobile-enabled population—IDC’s Worldwide Digital Marketplace Model and Forecast expects the number of mobile devices accessing the internet to surpass the one billion mark by 2013—presents security challenges to application providers. It may not be in the best interests of an organization to permit access to sensitive or confidential documents to mobile workers who are accessing corporate resources from a public or shared device. Similarly, it may be desirable to only permit access to resources from certain locations when the connection between the client and the resource is encrypted.

MSAs and DMAs are geographical boundaries ranging from countries down to specific U.S. metropolitan areas. There is extensive demographic information available for these areas and accurate geolocation data can determine which specific MSAs and DMAs are applicable to a given user based on the IP address from which they access an application.
In order to provide this kind of graded authentication and authorization of access to corporate resources based on user location, it is first necessary to ensure, as much as possible, that the gateway to those resources are capable of accurately determining the location of the client.

Accurate geolocation data, when combined with the other variables that make up a request’s context, can permit or deny application and resource access in an increasingly fine-grained manner. Geolocation information is one of the key pieces of contextual information surrounding requests that can be used to enhance and provide better enforcement of organizational security policies.

**Enhanced Visibility**

Just as accurate geolocation data has valuable benefits in terms of security and performance of web applications and resources, it also provides greater business value and insight through enhanced visibility. Business value and insight come from discerning the client’s location and from additional data provided by geolocation. For example, geolocation can be used in defined areas, such as those established by Designated Market Areas (DMAs) and Metropolitan Statistical Areas (MSAs), to derive deep demographic data that becomes part of the application request context and can be subsequently incorporated into analytical evaluation of visitor and customer web application interaction.

Understanding from where clients typically access your applications can influence the placement of future data centers and co-location of CDN components to improve application performance and distribution. Accurate geolocation data can assist in prioritization of requests by aligning application delivery policies with defined demographic-based business goals.

Data such as the time zone associated with visitors, typically available through provider geolocation data, can further assist IT in gaining visibility into use patterns based on time. This visibility affords an opportunity to understand the potential impact of leveraging cloud computing and employing a “follow the users” strategy for improving application performance, potentially eliminating the need to provision costly CDN services. Moving the content closer to the users is still a valid strategy, but knowing the application access point for the majority of customers makes it possible to move the entire application across cloud computing environments rather than add additional complexity with a CDN service.

Business analysts understand the value derived from demographics, especially those based on location. But the demographics that are typically analyzed using
business intelligence tools are only for customers with known locations. However, demographics provided via geolocation for visitors can be correlated with data on known locations to provide insight as to why those visitors have not become customers. This information is invaluable to business analysts when determining, for example, which products are not selling well in a particular location but may be of interest, or in understanding the impact of location on visitor interaction with web applications.

Geolocation Implementation

Geolocation integration can be accomplished at many different points in an application request’s lifecycle. To realize the greatest value across the broadest spectrum of use cases, gathering of geolocation data is most efficiently accomplished when a request is first made for a given resource.

The Application Delivery Controller is typically deployed at a strategic point in the application and network architecture: at the perimeter of the network, acting as an intermediary between clients and resources. Given this strategic location, geolocation data should be incorporated into the existing context that is already associated with every request such as IP address, user-agent, and ability to accept specific types of content.

Accurate geolocation data is generally provided by an external, third-party service. These services can be billed in a variety of ways, including by the number of queries and bandwidth transferred. To minimize the capital and operational costs associated with retrieving geolocation data while maintaining the ability to share that data with the broadest number of devices and applications, centralization of the retrieval process is necessary. Centralized control has the added benefit of decreasing organizational risk by permitting or denying access at the perimeter of the network when location is part of the authorization process.

By integrating geolocation services with a unified application delivery service, it is also possible to share the data retrieved from the third-party service with all functions deployed on the Unified Application and Data Delivery platform. A unified application delivery platform shares a core, underlying traffic management system that enables the sharing of request context—including location data—across all modules that are deployed on that platform. The sharing of contextual data enables web application security, access management, acceleration, and core load balancing services on the application delivery platform to take advantage of the geolocation
data available via the global server load balancing component, which is generally the component through which geolocation services are provided.

Conclusion

Accurate geolocation data is often viewed as useful only in certain scenarios involving CDNs and advertising efforts. The increasingly global nature of content and the migration of multimedia content distribution from typical broadcast channels to the Internet make geolocation a requirement for enforcing access restrictions and for providing the basis for traditional performance-enhancing and disaster recovery solutions.

Both business and technical stakeholders will find value and a broad range of uses for the highly accurate data available from a trusted third-party geolocation provider, especially when the data is integrated into a Unified Application and Data Delivery platform.