Geolocation is a technology that uses data acquired from an individual’s computer or mobile device to identify or describe the user’s actual physical location. Two types of data can be collected—active user/device-based information and passive server-based lookup/data correlation—and then cross-referenced against each other to create the most accurate result.

There are three main categories of geolocation data, as shown in figure 1.

Geolocation makes it possible, from any device connected to the Internet, to obtain all types of information in real time and locate the user with pinpoint accuracy at a given point in time. Geolocation technology is the foundation for location-positioning services and location-aware applications (apps). With the number of smartphone users expected to reach 2.66 billion by 2019 and more than 2 million apps available in both the Android and iPhone markets, the prevalence of geolocation technology will only continue to increase.

Geolocation data have a variety of uses, each of which can be tailored to particular apps, environments or enterprises. These uses presently include localization and/or customization of delivered content, enforcement of access and delivery restrictions based on geographical location, fraud prevention, and network traffic analysis. Extending these technologies and their demand entails extending the problem of the nature of the information—often private and/or sensitive—associated with them. It is, therefore, important to be especially aware of issues relating to security and privacy to be able to use geolocation tools responsibly.

**Impacts of Geolocation**

The proliferation of Global Positioning Systems (GPS), Wi-Fi, wireless mobile networks and IP location identification techniques makes a wide range of derivative technology applications possible: tailoring content and services to users in particular locations, conducting financial transactions from mobile devices with greater assurance of wireless security, and leveraging the ability to use cloud storage to synchronize devices across a multitude of mobile platforms and varying user locations. The capability to provide accurate and timely georeference data, tag items of interest with location metadata, and use location coordinates as a key to search databases is the foundation for a thriving software market for applications that run on mobile platforms.

Consequently, it is also now possible to enhance and control Internet commerce by using geolocation information to provide virtual boundaries and *de facto* controls for activities such as Internet gambling, video distribution, and procurement of products and services that may be restricted in one jurisdiction, but permitted in another. However, such boundaries and controls can be intentionally

---

**Betsie Estes**

Is a research manager with ISACA and has been with the association for five years.

---

<table>
<thead>
<tr>
<th>Type of Geolocation Data</th>
<th>Description of Use</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Georeferencing or positioning</td>
<td>Ascertaining the physical location of an object/person relative to a map</td>
<td>Monitoring a prisoner via Global Positioning System (GPS)-enabled ankle bracelets</td>
</tr>
<tr>
<td>Geocoding</td>
<td>Searching for information regarding objects or services on a map</td>
<td>Locating a particular type of restaurant or retail establishment</td>
</tr>
<tr>
<td>Geotagging</td>
<td>Adding geographic location information to an object</td>
<td>Checking in at a restaurant via social media</td>
</tr>
</tbody>
</table>

evaded using web proxies or anonymizer software. Of course, coinciding with these benefits is a range of social and privacy considerations on how geolocation data, when correlated with other personally identifiable information (PII), can be used or abused.

As with any technology, geolocation has a double-edged nature. The capabilities that empower social networking, aid in law enforcement, and transform the way the world is experienced and navigated also provide the basis for serious misuse in the wrong hands. Such misuse includes unwarranted surveillance of individual or enterprise activities and use in criminal activities. In addition, there are easily available tools that enable intentional evasion of geolocation—an ability that may facilitate criminal acts.

**Business Benefits of Geolocation**

The business benefits of geolocation are far-reaching and are being leveraged by all types of enterprises—manufacturing, retail, financial services, insurance, transportation, utilities and governments. As business and government services are enhanced, the user or consumer of those services benefits as well. Some business benefits and uses include:

- Targeted advertising
- Delivery and asset management, e.g., truck location and manifest status
- Content customization and delivery
- Augmented reality
- E-discovery in support of litigation and regulatory enforcement
- Autonomous vehicles
- Load balancing
- Fraud detection and prevention using Internet protocol (IP) location technology in conjunction with fraud profile data
- Real-time incident management through geolocation enrichment of logs and other IT data

For many businesses, the use of geolocation and mobile technologies is critical to success. Geolocation in conjunction with cross-platform mobile applications provides the basis for enhanced customer experiences and presents opportunities for enterprises to merge location with social media-based and other information into context-enriched services.

**Risk, Security and Privacy Concerns of Geolocation**

Mobile geolocation services are pervasive in the “always connected” world. They have introduced innovative, profitable and functional services and applications. With location technology, a user’s experience can be uniquely personalized, which appeals to marketers, retailers, government entities, law enforcement, lawyers and, unfortunately, criminals. Despite their many benefits, these services do increase risk to the user, the service providers and those who utilize the data collected by the service providers.

The potential benefits have led many individuals and enterprises to adopt this technology, resulting in more data and personal privacy risk in the virtual network and an exponential increase in the inherent vulnerability for geolocation data across the information life cycle. When someone utilizes an app and its services, there may be multiple data controllers: the service provider, wireless access points and/or developers. Multiple data controllers force users to accede control of the systems...
that determine and store their location and other personal information. Consequently, users usually cannot identify the source and ownership of data collection. This raises several concerns for users such as how their location data are being used, with whom the data will be shared, whether there will be onward transfer of the data, and the timeline for data retention and destruction. As the use of location-aware apps and geomarketing becomes increasingly pervasive, concerns continue to exist around online privacy—specifically, business practices around the collection and use of the PII.

As the user group grows, continually utilizing new features and creative apps on their mobile devices, the prospect of criminal attacks becomes even more worrisome. Each user’s personal information, including race, gender, occupation and financial history, has significant financial value. Therefore, location information is of particularly high value. Information from a GPS and geolocation tags, in combination with other personal information, can be utilized by criminals to identify an individual’s present or future location, thus facilitating the ability to cause harm to individuals and/or their property, ranging from burglary and theft to stalking, kidnapping and domestic violence. And the risk of identity theft increases with each collection of PII, especially when the information is not maintained for the purpose of specifically identifying an individual. Technology that can match PII with a user’s location presents an additional layer of privacy concern. In this climate, companies need to think carefully about their geomarketing practices and examine whether their current privacy policies accurately reflect the collection and use of geolocation data.

Criminal activity can take various forms. Physical crime, while more visceral, is likely less prevalent than cybercrime. Major corporations usually store positional data on remote servers. Through IP geolocation data, a user’s physical location and computer can be identified. Using GPS on a computer or mobile device and geolocation tags on pictures and video also reveals personal information such as home, work and school addresses and a daily itinerary. A cybercriminal then can mine personal information (e.g., credit card numbers and government identification numbers) by utilizing social engineering, malware, key loggers and persistent threat mechanisms to steal a user’s identity.

Geolocation risk factors extend beyond the individual. The location data risk also pertains to enterprises, employees and families. The areas of concern regarding privacy and safety on geolocation are:

- What data are collected?
- Who is collecting location data and how are they used?
- With whom can the data be shared, and how long are they stored?
- Would accidental or unintentional sharing of location data result in annoyance, embarrassment or danger to an individual’s safety?

Concerns (such as those relating to transparency) about data collection practices, solicitations made based on geolocation data obtained without the user’s consent, and physical safety stemming from the misuse of information that can identify a user’s current (or future) physical location emphasize the sensitivity of geolocation data.

From a business perspective, geolocation data present a unique risk. For example, this type of location-based information can give a competitive advantage to business rivals. The knowledge that a group of executives is at a specific location could constitute unauthorized disclosure of confidential or proprietary business information, such as a merger, an acquisition, or a research and development breakthrough. This type of breach
can affect reputation, brand strength and financial statements. For employees, there is a risk of their employers utilizing geolocation data to monitor them both during and outside of work hours. There may be a justifiable business reason, e.g., to identify and locate delinquent employees, but it could also extend into a gray area, such as tracking an employee's recreational activities because the company believes they may negatively affect its reputation. Enterprises collecting and/or using geolocation data face a difficult task in balancing the privacy and ethical use concerns of customers, employees and other individuals with challenges and opportunities posed by geolocation information.

**Strategies for Addressing Risk Associated With Use of Geolocation**

There are two paths that can mitigate the risk of geolocation: through technology safeguards and through the user.

The geolocation provider and other third parties must implement the appropriate safeguards and a privacy and security governance program. Enterprises should not view privacy as a regulatory hurdle to jump. The program implemented should be proactive. The enterprise must educate itself and adhere to any applicable regulations, guidelines and standards. Each department within an enterprise should proactively manage the inputs and outputs of the technology and provide input on the strategy.

The appropriate general controls should be implemented within the geolocation technology. For instance, the operating system and software should be updated periodically, patches should be implemented and backups should be performed regularly. In addition, there should be logical physical access controls that restrict access to a need-to-know basis and are monitored for unauthorized access. In addition, subscribing to the principle of “keep the least for the shortest period” and using anonymization techniques are recommended. These pervasive controls may not directly impact safeguarding PII, but they are extremely important and provide the foundation for a strong defense-in-depth technology infrastructure.

Another extremely important task is data classification. Without knowing where the data are, who owns the data and the source of the data, the data cannot be appropriately safeguarded. Through data classification, the enterprise should identify the data that are considered personal information and confirm that there are appropriate mechanisms, such as encryption, to mitigate the risk of disclosure. In addition, data that are considered personal information should be either redacted or anonymized. Appropriate integrity controls should be used in the event location data and associated PII may be required for discovery or forensics purposes.

An enterprise should verify that it is adhering to its privacy policy for location-based services. The enterprise may be liable for deceptive or unfair business practices if it utilizes the collected data for a purpose not included within the notice. Therefore, the enterprise should confirm its documented guidelines regarding notice, choice and onward transfer to validate that its practices are in sync with its notice.

The enterprise then needs to design a governance framework to address privacy and security implications. The framework should use a top-down approach and be pervasive for the entire enterprise. First, the enterprise needs to identify the strategy it is going to implement for geolocation. The strategy should be linked to other technologies and follow the
same privacy and security standards for safeguarding personal information. Second, depending on the strategy, policies and procedures, consistent nomenclature should be implemented and followed. Third, communication, training and awareness programs should be established to educate the user, developer and other parties who will collect or use the data. Last, a monitoring and reporting structure should be put in place to proactively manage issues, breaches and exceptions.

There are important questions that an organization should ask which should be part of an organization's factual due-diligence process when dealing with data from users: knowing what the location-aware application does; what type of data it collects; and whether the data are shared with affiliates, partners or third parties. An organization should pose the right questions regarding which data are aggregated, if it can identify an individual, which are the data flows from its location-aware offering and if it will share data with other parties.

In addition to safeguards implemented at the geolocation organization, users must also play a key role in safeguarding their personal information. As a first step, users should identify within the application or service how to disable, opt out and understand the capabilities of the technology.

Also, users should educate themselves and increase awareness among others on geolocation data because the actions of families, friends and coworkers may disclose location-based information users wish to be kept private. For example, social media tagging capabilities may inadvertently identify an individual and disclose associated geolocation data. As users become more aware and understand the corresponding risk, ideally, they will begin to think carefully before posting or tagging personal information. It will require a collaborative effort between enterprises and users and a shift in behavior to maintain privacy in a digital world.

Governance and Change Consideration for Use of Geolocation

Geolocation technology in and of itself is neutral. Of greater importance is how geolocation data are acquired, used and archived. In this sense, governance pertains more particularly to how capabilities implicit in a specific geolocation technology are used, how geolocation services manage geolocation data to comply with relevant laws and regulations, and how the interests of the objects of geolocation (such as individuals) are served and protected.

At the heart of an enterprise’s governance activity is the mechanism by which geolocation information is ethically used and protected.

From a legal or regulatory perspective, governance of geolocation is a matter of how to address opt-in or opt-out privacy rules, depending on jurisdictional rules and boundaries. Opt-in and opt-out are the two options the user or subscriber can have to manage the degree of privacy in mobile devices. The opt-in system requires a previous action by the user, i.e., informed consent and authorization, to begin the collection of location and/or provision of location services by a third party. The opt-out system considers location service active by default and, as such, requires the user to execute an action later to deactivate it. The former is the approach taken by the European Union, whereas the latter is the prevailing situation in the United States.

Assurance Considerations Pertaining to Geolocation

There are four assurance aspects related to geolocation technology and its use:

- Introduce the COBIT® 5 framework for use by service providers and requesters to provide the basis for risk management and proper use of data.
• Audit, vet and certify geolocation service providers and third-party users. Such audits and certification can take the form of, for example, International Standards for Assurance Engagements (ISAE) 3402 (or Statement on Standards for Attestation Engagements [SSAE] 16) reports and trusted third-party branding, such as TRUSTe evaluations.

• Provide a security and safety assessment of mobile applications employing geolocation capabilities.

• Ensure compliance with privacy and usage laws and regulations by service providers and technology developers across diverse international jurisdictional boundaries.

Some specific considerations relating to geolocation that an assurance strategy should address include:

• The integrity of underlying technologies as manufactured and the associated integrity of geolocation service infrastructures utilizing or depending on those technologies. This includes the integrity of the geolocation data records and the audit trail records of the underlying infrastructure.

• User behavioral analysis and profiling to ascertain the degree of compliance and effectiveness of user data protection safeguards in a variety of scenarios.

• Privacy protection assurances, such as use of privacy by design methods and secure database technologies to protect against unauthorized collection of, access to or improper use of sensitive personal information associated with geolocation data.

• Proper policies, processes and procedures governing an enterprise’s use of third-party geolocation services and data and related ethics of use guidelines and requirements.

• Awareness training for all employees regarding the implications, benefits and associated responsibilities involved in the collection and use of geolocation information.

• Vetting of third-party software application developers and software to:
  – Ensure software security and integrity through secure application design and test methodologies
  – Require the use of trusted platforms and tool sets for application development
  – Adhere to secure systems development life cycle (SDLC) processes and procedures

Conclusion

As the sophistication of geolocation technologies increases, along with the diversity of services built on them, there will be recurring topics and themes that society will continue to consider and debate.

Those concerns include how mobile devices, networks and location-based services have changed values regarding privacy, data collection and data use. Some other questions for consideration include: What rights do people and organizations have regarding data that are collected? What rights do people and organizations expect, and are these expectations changing as services become more popular? What rights are granted and recognized internationally, and how can compliance with local and international standards be assured? What rights should corporations ethically grant their users? Who is responsible when a breach occurs? Is true anonymization even possible in today’s increasingly connected world?

Finding answers to these and other questions in the future should prove challenging yet enlightening.

Endnotes


5 Enterprises should consult COBIT 5 for more information on designing a governance framework, available at www.isaca.org/cobit/pages/default.aspx.