An
ISACA
White Paper

ISACA®
Trust in, and value from, information systems

Geolocation: Risk, Issues and Strategies

Abstract
Geolocation data, revealing an individual's physical location, are obtained using tracking technologies such as global positioning system (GPS) devices, Internet Protocol (IP) geolocation using databases that map IP addresses to geographic locations, and financial transaction information. Uses of the information are myriad, including direct marketing and context-sensitive content delivery, monitoring of criminals, enforcing location-based access restrictions on services, cloud balancing, and fraud detection and prevention. Geolocation technologies and their application, while offering social and economic benefit to a mobile society, raise significant privacy and risk concerns for individuals, businesses and governments.

ISACA®

With 95,000 constituents in 160 countries, ISACA (*www.isaca.org*) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, the nonprofit, independent ISACA hosts international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations. ISACA continually updates COBIT®, which helps IT professionals and enterprise leaders fulfill their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

Disclaimer

ISACA has designed and created *Geolocation: Risk, Issues and Strategies* (the "Work") primarily as an educational resource for security, governance and assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, security, governance and assurance professionals should apply their own professional judgment to the specific control circumstances presented by the particular systems or information technology environment.

Reservation of Rights

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: *info@isaca.org*
Web site: *www.isaca.org*

Geolocation: Risk, Issues and Strategies

Acknowledgments

ISACA wishes to recognize:

Project Development Team
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, 6 Sigma, Quest Software, Spain
Avani Mehta-Desai, CISA, CRISC, KPMG LLP, USA
Rodolfo Tesone, ICT Law Section, Bar Association of Barcelona, Spain
Jonathan Wilson, CISA, CIA, CEH, Advantage Health Solutions, USA

Expert Reviewers
Sourabh Awasthi, TCS, USA
Nadeem Bukhari, CISM, CISSP, Kinamik Data Integrity, USA
Roger Gallego, Entelgy, Spain
Albert llado, CISA, CISM, CGEIT, CRISC, Auren International, Spain
Pablo Ruiz Muzquiz, Kaleidos, Spain
Gorka Sadowski, CISSP, LogLogic, Spain
Michael Yung, CISA, CISM, Next Media, China

ISACA Board of Directors
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, International President
Christos K. Dimitriadis, Ph.D., CISA, CISM, INTRALOT S.A., Greece, Vice President
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Vice President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Vice President
Niraj Kapasi, CISA, Kapasi Bangad Tech Consulting Pvt. Ltd., India, Vice President
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management, Inc., USA, Vice President
Jo Stewart-Rattray, CISA, CISM, CGEIT, CSEPS, RSM Bird Cameron, Australia, Vice President
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd., USA, Past International President
Lynn C. Lawton, CISA, FBCS CITP, FCA, FIIA, KPMG Ltd., Russian Federation, Past International President
Allan Neville Boardman, CISA, CISM, CGEIT, CRISC, CA, CISSP, Morgan Stanley, UK, Director
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Belgium, Director

Knowledge Board
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Belgium, Chairman
Michael A. Berardi Jr., CISA, CGEIT, Nestle USA, USA
John Ho Chi, CISA, CISM, CFE, CBCP, Ernst & Young LLP, Singapore
Phil Lageschulte, CGEIT, CPA, KPMG LLP, USA
Jon Singleton, CISA, FCA, Canada
Patrick Stachtchenko, CISA, CGEIT, Stachtchenko & Associates SAS, France

Guidance and Practices Committee
Phil Lageschulte, CGEIT, CPA, KPMG LLP, USA, Chairman
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, 6 Sigma, Quest Software, Spain
Meenu Gupta, CISA, CISM, CBP, CIPP, CISSP, Mittal Technologies, USA
Yongdeok Kim, CISA, IBM Korea Inc., Korea
Gary Langham, CISA, CISM, CGEIT, CISSP, CPFA, Australia
Perry Menezes, CISM, CRISC, Deutsche Bank, USA
Mario Micallef, CGEIT, CPAA, FIA, Advisory in GRC, Malta
Salomon Rico, CISA, CISM, CGEIT, Deloitte Mexico, Mexico
Nikolaos Zacharopoulos, Geniki Bank, Greece

Acknowledgments *(cont.)*

ISACA and IT Governance Institute® (ITGI®) Affiliates and Sponsors
American Institute of Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association for Corporate Governance Inc.
FIDA Inform
Information Security Forum
Institute of Management Accountants Inc.
ISACA chapters
ITGI Japan
Norwich University
Solvay Brussels School of Economics and Management
Strategic Technology Management Institute (STMI) of the National University of Singapore
University of Antwerp Management School
ASI System Integration
Hewlett-Packard
IBM
SOAProjects Inc.
Symantec Corp.
TruArx Inc.

Introduction: What Is Geolocation and How Does It Work?

Stated simply, geolocation is a technology that uses data acquired from an individual's computer or mobile device (any type of radio or network-connection-enabled device) to identify or describe his/her actual physical location. It is one of the most popular manifestations of the current development of information technologies and is recently experiencing a significant rise in popularity.

A more systems-oriented definition might be as follows:

> *A geolocation system is an information technology solution that ascertains the location of an object in the physical (geo-spatial) or virtual (Internet) environment. Most often, the object is a person who wants to utilize a service based on location, while maintaining his/her privacy.*

Geolocation software services are used to support the business objectives of private and public enterprises.

Geolocation data generally are used for three purposes:[1]
- **Geo-referencing or positioning**—Ascertaining the physical location of an object or person relative to a coordinate system (map) to access specific information later. Examples of this are car navigation via a global positioning system (GPS) device such as TomTom™ and prisoner monitoring via GPS-enabled ankle bracelets.
- **Geo-coding**—Searching for information regarding objects or services on a map, such as locating a restaurant offering a particular type of cuisine
- **Geo-tagging**—Adding geographic information to an object, such as a photograph, by incorporating the geolocation data in the photograph's metadata

Geolocation makes it possible, from a device connected to the Internet, to obtain various types of information in real time and locate it on the map with high accuracy at a given point in time. Geolocation data can be collected in a multitude of ways: web browsing via IP addresses, mobile phones, GPS devices, radio frequency identification (RFID), credit/debit card transactions, tags in photographs, and postings (such as geo-tags or check-ins using applications such as Foursquare) on social network sites such as Facebook® and Twitter. Geolocation technology has become a foundation for location-positioning services and location-aware applications running on smartphones such as iPhone® and Android™ devices.

Geolocation data have a variety of uses, each of which can be tailored to particular applications, environments or enterprises. These uses presently include localization and/or customization of delivered content, enforcement of access and delivery restrictions based on geographic location, fraud prevention, and network traffic analysis.[2] Extending these technologies and their demand entails 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.

Geolocation data is generated and collected in one of two ways—in an active mode referred to as user-device-based geolocation or in a passive mode referred to as table look-up or data correlation server-based geolocation. **Figure 1** summarizes these modes and the technologies each employs.

[1] See, for example, San-Jose, Pablo; Cristina Gutierrez Borge; Eduardo Alvarez Alonso; Susana de la Fuente Rodriguez; Laura Garcia Perez; *Guide to Security and Privacy of Geolocation Tools*, Information Security Observatory, INTECO, Spain, 2011

[2] King, Kevin, "Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Geolocation Technologies," *Albany Law Journal of Science and Technology*, January 2011

Figure 1—Modes of Geolocation Data Generation and Collection		
Mode	**Collection Method**	**Technologies Involved**
Active: User—Device-based	• Uses firmware and software on user's computer or wireless device • Location determined via GPS chip and/or triangulation using cellular tower information • Request-response model	• GPS • Assisted GPS (A-GPS) • Wi-Fi—Wireless positioning • 3G/4G • Mobile applications—iPhone, Android devices, BlackBerry®
Passive: Data-lookup—Sever-based	• Involves use of third-party geolocation service providers, e.g., Quova®, NetGeo, Bering Media • Based on nonlocation-specific IP address acquired from user device or service set identifiers (SSIDs) for wireless networks • Correlation with stored IP or SSID databases obtained from purchase records, user-provided information, network analysis of trace routes and domain name system (DNS) host names	• IP location—*Whois* lookup, DNS LOC, geographic names in domain name user or application information, timing data using ping inference based on routing data, e.g., *traceroute* monitoring of Internet service provider (ISP) networks • 3G/4G • Wi-Fi—Wireless positioning

Impacts of Geolocation

The capability to provide accurate and timely geo-reference data, tag items of interest with location metadata, and use location coordinates as a key to search databases has become the foundation for an expanding software market for applications that run on mobile platforms.

The advent of GPS, Wi-Fi, wireless mobile networks and IP location identification techniques has spawned a wide range of derivative technology applications. These include the ability to tailor content and services to users in particular locations; conduct financial transactions from mobile devices with greater assurance of detecting fraud; and apply new uses for cloud computing paradigms, such as using cloud storage to synchronize heterogeneous devices in support of context-aware computing across a multitude of mobile platforms and varying user locations. The capability to provide accurate and timely geo-reference data, tag items of interest with location metadata, and use location coordinates as a key to search databases has become the foundation for an expanding software market for applications that run on mobile platforms.

Consequently, it has become 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 evaded by using web proxies, anonymizer software, e.g., Tor, or Internet services such as My Expat Network. Of course, concomitant 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. These privacy and related security matters are discussed in a later section of this publication.

As with any technology, geolocation has a double-edged nature. The capabilities that empower social networking, aid in law enforcement, and transform how the world is experienced and navigated and 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 tools, such as the anonymizer Tor, 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 sales, 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 include:

The business benefits of geolocation are far-reaching and are being leveraged by all types of enterprises—manufacturing, retail sales, financial services, insurance, transportation, utilities and governments.

- In advertising, use of designated market areas (DMA) and demographic data, e.g., from metropolitan statistical areas (MSA)
- Know your customer (KYC), e.g., better understanding of customer requirements and expectations for products and services and benefits accruing from targeted sales
- Delivery and asset management, e.g., truck location and manifest status
- Content customization and delivery, such as movies on demand
- Augmented reality, i.e., the use of geo-reference data and other detection methods, such as motion sensors and compass, combined with virtual information from the Internet, to enrich the user's world view
- Fine-grained management of Internet commerce activities and interests
- E-discovery in support of litigation and regulatory enforcement
- Highway toll devices, e.g., I-Pass, EZ-Pass® in the US
- Vehicle *Ad Hoc* Networks (VANS), as used in the EU
- Optimal request routing
- Cloud balancing
- Fraud detection and prevention using IP location technology in conjunction with fraud profile data
- Real-time incident management through geolocation enrichment of logs and other IT data

Companies recognize the benefits of "geo-marketing" and the applications (apps) that can bring discounts and promotions directly to the user at the point of purchase and provide valuable, real-time data about customer preferences. These data can be used, in aggregate, to provide data on key market trends, or integrated into a customer profile to provide a more personalized experience. It would be difficult to compile this type of information through a more efficient process using any other currently known technology. Consumers benefit, too—from access to information that can be instantly relevant to a purchasing decision, to location-specific discounts and services.

For businesses, being on the vanguard of the use of geolocation and mobile technologies will be critical to future success. Geolocation in conjunction with cross-platform mobile applications will provide the basis for enhanced customer experiences and present 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 have become 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 a user utilizes an application 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 questions of concern for the user, 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 rise in the use of location-aware apps and geo-marketing continue, concerns keep on growing around online privacy—specifically, business practices around the collection and use of the PII data.

As the user group grows, continually utilizing new features and creative applications on their smartphones and other mobile devices, the prospect of criminal attacks becomes even more worrisome. The amount and the nature of individual and corporate information available to potential hackers would allow targeted attacks that are difficult to prevent, detect and manage.

In addition, each user's personal information, including race, gender, occupation and financial history, has significant financial value. Therefore, location information is particularly of 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 an individual and/or his/her 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. Regulators are aware of such concerns and are moving quickly to enact rules regarding how companies can use geolocation data. In this climate, companies should think carefully about their geo-marketing practices and examine whether their current privacy policies accurately reflect the collection and use of geolocation data.

Companies should think carefully about their geo-marketing 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 Social Security or other government identification numbers) by utilizing social engineering, malware, key loggers and persistent threat mechanisms to steal a user's identity.

From social engineering arises the risk of a user being subjected to location-based spamming. IP geolocation attacks in two ways:
- It identifies the physical location of an organization's hosted e-mail. The spammer uses this information to plan a targeted attack that will overload the enterprise's servers, causing usage issues.
- Spamming attacks to an individual's e-mail or mobile device are targeted and are, therefore, highly effective at soliciting a response acknowledgment from the victim.

Geolocation risk extends farther than to a sole 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? How are the data used? With whom can the data be shared? How long can the data be stored?
- Spamming by advertisements or offers based on physical location
- Accidental or unintentional sharing of location data resulting in annoyance, embarrassment or danger to an individual

Consequently, there is a growing consensus that geolocation data should be classified as sensitive due to a number of concerns such as 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.

Geolocation data can give a competitive advantage to business rivals. For example, 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. Employees face the 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.

There is a growing consensus that geolocation data should be classified as sensitive due to a number of concerns such as 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.

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. As an enterprise considers how to integrate geolocation into its services and offerings, an ISACA developed model, the Business Model for Information Security (BMIS) can be applied to assist in developing an optimal balance among the competing concerns regarding geolocation. BMIS provides a means to examine the interrelationships of the traditional triad of people, process and technology together with the cultural and organizational aspects of the enterprise as it develops a strategy for services and activities involving geolocation data use and protection.

Strategies for Addressing Risk Associated With Use of Geolocation

Current law does not articulate a stance on the privacy and security aspect of geolocation. Therefore, it is uncertain whether enterprises have a legal obligation to the users and developers of the geolocation data. Yet, despite legal guidelines or absence thereof, there are two paths that can mitigate the risk of geolocation: through technology safeguards and through the user. There is an implied urgency in addressing such risk as the geolocation genie is out of the bottle, so to speak.

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. Therefore, the enterprise needs to educate itself on what is needed in the absence of a legal mandate, audit guidelines or standards, or the presence of confidentiality risk. 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 with antivirus software, patches should be implemented and backups should be performed regularly. In addition, there should be logical and 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" as well as using anonymization techniques is recommended. These pervasive controls may not directly impact safeguarding of personal information, but they are extremely important and provide the foundation for a strong defense-in-depth technology infrastructure.

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.

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 that 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, procedures and 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.

As noted earlier, ISACA's BMIS can be of use to enterprises wrestling with the question of how to address the context and protection of geolocation information within the enterprise. In addition, ISACA's Risk IT (and Val IT) and COBIT frameworks can be applied to develop a risk mitigation (and value-chain) strategy and privacy compliance and protection processes pertaining to the collection, use and governance of geolocation information.

There are important questions that a company should ask and that should be part of a company'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 those data are shared with affiliates, partners or third parties. An organization should pose the right questions regarding which data are aggregated, whether the data can identify an individual, what are the data flows from its location-aware offering, and whether the organization will share data with other parties.

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

Users also should also educate themselves and increase awareness among others on evolving technologies. As users become aware and begin to understand the corresponding risk, it is hoped that they will think carefully before posting or tagging personal information. It will require collaborative effort between the enterprise and the user, and a shift in user behavior, to maintain privacy in a digital world. Users should also educate families, friends and coworkers as their actions may disclose location-based information that a user wishes to be kept private. For example, Facebook's facial recognition technology and/or tagging capabilities may inadvertently identify an individual and disclose associated geolocation data. This type of collaboration and shift in behavior will necessitate that the user reexamine how to maintain one's 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. Privacy and the protection of PII are key considerations, together with how such information is collected and used. In legal or regulatory parlance, 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 with 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 EU, whereas the latter is the prevailing situation in the US.

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

It is also important to note the close relationship developed between geolocation technologies and social networks, collaborative communities, and other services related to the so-called Web 2.0. Users have the opportunity to integrate virtually any kind of geo-referenced information on popular social networks as well as using new specially designed social networks that are developed on geolocation technology. The use of appropriate countermeasures and security mindset applies here as indicated in ISACA's recent white paper entitled *Social Media*.

Assurance Considerations Pertaining to Geolocation

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

- ISACA's Risk IT and COBIT frameworks can be used by service providers and requestors to provide the basis for risk management, compliance and proper use of geolocation information.
- Auditing, vetting and certifying geolocation service providers and third-party users. Such audits and certification can take the form of, for example, ISAE3402 (or SSAE16) reports and trusted third-party branding such as VeriSign®, TRUSTe® and Common Criteria (CC) Target of Evaluation (TOE) evaluations.
- Providing security and safety assessment of mobile applications employing geolocation capabilities, e.g., iPhone applications, Android applications, and proper use of HTML5 and other geolocation-related application programming interfaces (APIs). The ISACA white paper *Securing Mobile Devices* provides useful information in this regard.
- Ensuring compliance with privacy and usage laws and regulations by service providers and technology developers across diverse international jurisdictional boundaries. Compliance in this context would also include consideration of the full spectrum of ethics of use issues.

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

- 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
- 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.
- Security of client-side devices including susceptibility to man-in-the-middle (MIM) attacks, packet sniffing and signal-/frequency-based attacks
- 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
- Awareness training for all C-level and executive management 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 to address data-caching concerns, covert use of location data in metadata, and protection against the range of web-based attacks.
  - Require the use of trusted platforms and tool sets for application development to reduce risk from viruses, malware, unauthorized operating system (OS) modifications and misuse of open APIs.
  - Adhere to secure systems development life cycle (SDLC) processes and procedures such as configuration management by in-house or third-party application developers.

Conclusion

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, supporting fraud prevention, and providing the basis for traditional performance-enhancing and disaster recovery solutions.

Accurate geolocation data are often viewed as useful only in certain scenarios involving content delivery networks and advertising efforts. As recently noted by a network supplier,[3] "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, supporting fraud prevention, and providing the basis for traditional performance-enhancing and disaster recovery solutions."

As the sophistication of the geolocation technologies themselves 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, such as those put forth at a recent symposium on mobile devices, geolocation and shifting values, sponsored by Fordham University:[4]

- How do mobile devices and location technologies impact the distribution of content? How does mobile computing impact intellectual property rights? What challenges do content providers face in bringing their products to mobile devices? How do these challenges vary across national borders? How does mobility impact distribution rights? How do location technologies impact territorial licensing and royalty calculations?
- How have mobile devices, networks and location-based services changed our values regarding privacy, data collection and data use?
- What rights do people and organizations have regarding the data 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?
- What standards should apply to government access to, and collection of, location data? What limits should there be on law enforcement access to these data? What are the most significant international differences in the standards for government access to location data?

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

[3] MacVittie, Lori; *Geolocation and Application Delivery*, F5 White Paper, USA, 2010
[4] "Fifth Annual Law and Information Society Symposium: Mobile Devices, Technologies and Shifting Values," Fordham University, USA, 25 March 2011

Additional Resources and Feedback
Visit *www.isaca.org/geolocation* for additional resources and use the feedback function to provide your comments and suggestions on this document. Your feedback is a very important element in the development of ISACA guidance for its constituents and is greatly appreciated.