[GS-01-004] Location Privacy

Abstract

How effective is this fence at keeping people, objects, or sensitive information inside or outside? Location Privacy is concerned with the claim of individuals to determine when, how, and to what extent information about themselves and their location is communicated to others. Privacy implications for spatial data are growing in importance with growing awareness of the value of geo-information and the advent of the Internet of Things, Cloud-Based GIS, and Location Based Services.

In the rapidly changing landscape of GIS and public domain spatial data, issues of location privacy are more important now than ever before. Technological trailblazing tends to precede legal safeguards. The development of GIS tools and the work of the GIS&T research and user community have typically occurred at a much faster rate than the establishment of legislative frameworks governing the use of spatial data, including privacy concerns. Yet even in a collaborative environment that characterizes the GIS&T community, and despite progress made, the issue of location privacy is a particularly thorny one, occurring as it does at the intersection of geotechnology and society.

Keywords: legal aspects, location, privacy, security

Author & citation

Kerski, J. (2016). Location Privacy. The Geographic Information Science & Technology Body of Knowledge (3rd Quarter 2016 Edition), John P. Wilson (ed.).
DOI: 10.22224/gistbok/2016.3.2

Explanation

1. Definitions The following three components of the definitions of privacy are critical to its understanding and its connections to GIS&T.

Privacy. The claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others (Westin 1970).

Location Privacy concerns the claim of individuals to determine when, how, and to what extent location information about them is communicated to others. It refers to the ability of an individual to move in public spaces with a reasonable expectation that their location will not be recorded without permission for later use by a third party (Kerski and Clark 2012). Location privacy is the right to not be subjected to unsanctioned collection, aggregation, distribution, or selling of an individual or organization's location or profile. It is the ability of an individual, group, or organization to conceal location information, or "the right to be left alone" (Barrett et al. 2013).

Privacy recognizes preferences of revealing location data in different forms (Krumm 2008):

- When – A subject may be more concerned about current or future location than past locations.
- How – A user may be uncomfortable with automated requests for location, but may be receptive to manual requests.
- Extent – A user may prefer that location be reported as a "region" rather than a specific point.

2. Importance of Location Privacy

2.1 Privacy issues are inherently personal, including rights, ownership, copyright, choice, consent, stalking, transparency, disclosure, crime, and access to proprietary information. Unlike other types of personal information, much about someone's identity may be inferred from location, a type of personally-identifiable information that is highly dynamic. This can mean the exact geographic location (in past or present time) of an individual person; where they are known to reside or be employed; or where any of their particular devices (cell phones, cars, computers, etc.) were or are known to be.

2.2 In the past, the general public has not expressed extensive concern about matters of location privacy (Krumm 2008). The ability to monitor and track detailed location information for tagged items, such as the use of radio frequency identification (RFID) technologies through microchips, has been a boon to the workflows of supply chain management, for example. Being able to quantify and qualify patterns of human movement trajectories is critical for urban planning, public health, and emergency management activities. However, privacy implications for these geographic and spatial data are receiving increased attention for several reasons, including that

- an increased number of applications, devices, and activities in people's everyday lives are becoming geo-enabled as geographic information technology continues to evolve toward cloud-based SaaS (Software as a Service) architectures;
- organizations and businesses are increasingly recognizing that people's locational information has value (commercial, research, other) and are collecting more of it; and
- accessing and using high resolution and near-real-time location information is becoming easier.

3. Reasons for Privacy Concerns Surrounding GIS&T

3.1 The ease of capture, storage, and analysis of digital data has substantially increased the likelihood that an individual's location data is available (Duckham and Kulik 2006). For example, location data is regularly recorded by and available through mobile devices, geotagged media, and IP addresses. Additional sources include retail consumer products, social media, location based apps, organization employee and customer data, health care records, security cameras, mobile enabled check in services, personal tracking devices, bus passes, web traffic cams, local searches, and many more.

Moreover, a SaaS model allows the data and maps to be shared and accessed much more broadly, with more opportunities for unauthorized access. Interconnected geo-enabled devices and applications are part of the Internet of Things (IoT), and an increasing amount of data is available in real time. Data is stored on web servers, where, unfortunately, illegal access via hacking jeopardizes the integrity and security of the information.

3.2 The supply of and access to location data have enabled new monitoring techniques to be developed, such as geofencing. Through geofencing, it is possible to detect when and where one enters or leaves a physical space, such as a public square or a back yard. This functionality can be extended via software to location-enabled devices, such as being able to keep UAVs from flying in restricted airspace, but the service raises location privacy concerns for monitoring the movement of individuals without their knowledge.

3.3 In indoor spaces, Building Information Modeling (BIM) systems generate detailed digital maps of the interiors of buildings. This is of concern for several reasons, including (1) the scale of the data for the interior of buildings is much finer in resolution than typical geospatial data has been produced and analyzed in the past, down to the level of a person's individual workstation inside their office, for example. Such maps may enable others to infer individuals' precise location at a given time of day or night.

3.4 Autonomous vehicle data have implications for the collection and use of personal location data. Since self-driving cars "know" where they and their passengers are, and because they are connected to networks, that knowledge may be accessible by others.

3.5 Because many users primarily value the convenience afforded by geo-enabled devices, they may be oblivious to, or nonchalant about, the privacy implications of the digital trail of location information they produce. People contribute to vast archives of data, often unintentionally, through the human sensor network. Although courts have generally ruled that location information voluntarily shared by a person traveling in public places is not entitled to privacy protections, they also recognize that a person does not automatically make public everything he or she does merely by being there. Federal acts provide

protection of privacy under specific circumstances, such as family education, criminal victimization, and electronic communication. The 1974 U.S. Federal Privacy Act states that "records on individuals by federal agencies must be for a lawful and necessary purpose." The GIS Code of Ethics (URISA 2003 and GISCI 2014) includes the GIS professional's duty to "allow individuals to withhold consent from being added to a database, correct information about themselves in a database, and remove themselves from a database."

4. Privacy Laws and Government Information

4.1 Much of privacy law limits the data that the federal government may gather and publish on private individuals. In the United States, Directive DoD 5240.1-R from 1982 regulates the collection, retention, and dissemination of information on persons by intelligence agencies. Some argue that such laws do not go far enough; others that they go too far; others that they require update for the digital age. The rise of private-sector GIS muddies the waters of privacy legislation. Open record laws, which specify the circumstances under which the public can access government data, compound privacy issues. These laws, like privacy laws, vary widely between and even within countries.

4.2 Mechanisms do exist for location privacy protection, including regulatory strategies and privacy policies. Regulatory strategies, or government rules on the use of personal information, include notice and transparency, consent and use limitation, access and participation, integrity and security, and enforcement and accountability, and privacy policies include trust-based agreements between individuals and whomever is receiving their location data. Substantial efforts have been put forth by entities such as the Internet Engineering Task Force (IETF) to develop mechanisms for attaching privacy policies to data. Protecting both intellectual property as well as personal data are the intention of techniques such as anonymity, ambiguity, obfuscation, and geomasking (Zhang et al. 2015). However, such tasks are extremely difficult to implement and manage across the dynamic and rapidly evolving global network of digital data, as evidenced by the failure of earlier initiatives like the Platform for Privacy Preferences (P3P) project to be widely integrated into Internet browser functionality.

4.3 As the largest collector of domestic personal information, the U.S. Federal Government must deal regularly with securing the privacy of the location data it collects. The U.S. Census Bureau collects locational data on individuals but follows protocols for protecting the data, such as data swapping and data aggregation, and following the "72-Year-Rule" for some individual data. The National Institute of Health and the Department of Justice regularly use sophisticated geomasking and other computational techniques to protect the confidentiality of their subjects while still being able to conduct valid spatial analysis of the data. This has been a matter of specific research development as well for social media data collections such as geo-located Twitter feeds (Wang and Sinnott 2016). Increasingly, those involved with the collection and dissemination of social science data sets, such as ICPSR, recognize the need to address location data specifically by enforcing data masking and aggregation.

5. Handling Personal Data in the GIS&T Community

5.1 Though regulations and laws exist to protect the privacy of location data, enforcement is problematic and adherence must be, in part, a component of individual and professional responsibility. The GIS Code of Ethics (published by URISA in 2003 and later adopted by the GIS Certification Institute) recommends that respect for privacy and respect for individuals be maintained as part of the obligations of GIS professionals to society. GIS educators have opportunities to instill awareness of and a sensitivity towards location privacy with their students.

5.2 The need for professional responsibility extends to the organizations within which professionals engage. The National Science Foundation has mandated that a data management plan be part of every project that it funds, and scrutiny of how well the proposed plan addresses matters of locational data protection are the purview of both proposal reviewers and program officers. Institutional Review Boards (IRB) at universities and agencies sanction the proposed data collection and curation practices of researchers, but the individuals in charge of the local IRB process may be largely unfamiliar with the nature of geospatial data. Having guidelines to help IRBs become more savvy about the issues of location data can help inform policies and practices.

5.3 Onsrud and his colleagues (1994) recommend adherence to eight fundamental principles in handling personal data within the context of GIS&T. Though the geo-technologies themselves have evolved significantly since that time, these guiding principles are still valid and relevant.

1. Collection limitation principle: Limits should exist on the collection of personal information. Collection should be lawful, fair, and with the knowledge and consent of the individual.
2. Data quality principle: Data should be relevant, accurate, complete, and up-to-date.
3. Purpose specification principle: The information's purpose should be stated upon collection, and subsequent uses should be limited to those purposes.
4. Use limitation principle: No secondary uses of personal information should exist without the consent of the data subject or by the positive authorization of law.
5. Security safeguards principle: Personal data should be reasonably protected by the data collector.
6. Openness principle: Developments, practices, and policies with respect to personal data should follow a policy of openness.
7. Individual participation principle: Data subjects should be allowed to determine the existence of personal data files and be able to inspect and correct data.
8. Accountability principle: Data controllers should be held accountable for complying with the guidelines.

References

Contingency Today (2009). Big Brother Has Got Bags of Potential. Contingency Today (August 24).

Curtis, A. J., Mills, J. W., and Leitner, M. (2006). Spatial Confidentiality and GIS: Re-engineering Mortality Locations from Published Maps About Hurricane Katrina. International Journal of Health Geographics 5:44.

Duckham, M. and Kulik, L. (2013). Location privacy and location-aware computing.

University of Melbourne, Australia. In Dynamic and Mobile GIS: Investigating Changes in Space and Time, edited by Roland Billen, Elsa Joao, and David Forrest. CRC Press, Chapter 3.

GIM International. (2010). One Billion Square Kilometers of Earth Imagery. News item from GIM International.

GIS Certification Institute (GISCI). (2014). GIS Code of Ethics.

GIS Talk. 2009. Toronto Data Goes Public — Free GIS Data.

Gonzalez, R. C., and Woods, R. E. (2008). Digital Image Processing. Upper Saddle River, NJ: Prentice Hall.

Krumm, J. (2008). A survey of computational location privacy. Personal and Ubiquitous Computing 13(6): 391-399.

Onsrud, H. J., Johnson, J. P., and Lopez, X. (1994). Protecting Personal Privacy in Using Geographic Information Systems. Photogrammetric Engineering and Remote Sensing LX(9): 1083–1095.

Thurston, J. (2010). “How Does Satellite Imagery Compare with Aerial Photography?” V1 Magazine (April 4).

Tobler, W. R. (1987). Measuring Spatial Resolution. Proceedings of Land Resources Information Systems Conference, Beijing, 12–16.

Tobler, W. R. (1988). Resolution, resampling, and all that. In H. Mounsey & R. F. Tomlinson (Eds.), Building Databases for Global Science: the proceedings of the First meeting of the International Geographical Union Global Database Planning Project (pp. 129-137). Hampshire, U.K.: Taylor and Francis.

Urban and Regional Information Systems Association (URISA). (2003). A GIS Code of Ethics.

Wang, S. and Sinnott, R. (2016). Privacy protection of large-scale trajectories. Computing and Information Systems, 4th Annual Doctoral Colloquium, Program and Proceedings. Department of Computing & Information Systems, The University of Melbourne.

Westin, A. F. (1970). Privacy and Freedom. London: The Bodley Head, Ltd., 508.

Zhang, S., Freundschuh, S. M., Lenzer, K., and Zandbergen, P A. (2015). The location swapping method for geomasking. Cartography and Geographic Information Science, 44:1, 22-34.