Data Confidentiality

Zakiria A. Jordan

Old Dominion University

GEOG 495

Professor Jennifer Whytlaw

December 11, 2025

Introduction

Data confidentiality in Geographic Information Systems is an issue that gains more and more significance with the wider application of the technology in different fields. GIS technology allows the gathering and analysis of geographical data, which can include sensitive personal information like the location of individuals, their health data, or even information about public infrastructure. Such data is useful for purposes such as urban planning, disaster response, and healthcare but also raises concerns regarding privacy.

With the development of GIS, so have the risks of keeping this information secure. Real-time data usage, including data collected from GPS and mobile devices, has made it easier to collect specific location data on individuals. This ease also brings about ease in misusing such data if it is not well protected. For instance, personal data would be exposed or re-identified if not well anonymized or encrypted.

Because of these concerns, there have been various guidelines and best practices developed to securely manage geospatial data by organizations and individuals. For example, the Washington State Department of Social and Health Services has drawn up some Geospatial Data Confidentiality Guidelines for keeping public health data confidential. The set of guidelines provides a very clear framework for maintaining privacy and preventing misuse. Recent research also emphasizes the importance of encryption, access controls, and data anonymization in protecting geospatial information from unauthorized access.

The increasing relevance of data confidentiality is also reflected in international regulations on privacy. Laws like the General Data Protection Regulation in Europe set a very high bar for how data, including geospatial data, should be handled with respect to privacy and security. As technology continues to evolve, the future of data confidentiality in GIS will be based on further refining these practices and creating new legal and technological frameworks that protect personal information. It does indicate the current state of data confidentiality in GIS, challenges faced in the past, the present solutions, and directions towards the future for safeguarding sensitive geospatial data.

Status of the field – past, present, future

Historically, GIS was used for general mapping purposes, and little sensitive data were handled; however, as applications have evolved, the need to protect personal data is increasingly evident. Many older applications in environmental and land-use mapping posed less of a risk to privacy. Today, though, GIS finds broad applications in areas dealing with confidential information, such as healthcare, which utilizes GIS for disease outbreak tracking and access to healthcare. This trend requires higher standards of data confidentiality.

The current state of the field depends on a mix of technological solutions and legal frameworks to guarantee data confidentiality. For example, anonymization and pseudonymization are two well-known techniques in practice that can reduce some of the risks of exposing personal data. Regulation such as the General Data Protection Regulation (GDPR) has created a model in

Europe for how geospatial data must be treated, and such laws are developing globally. These frameworks thus try to balance between the utility of GIS data for public good and the privacy rights of individuals.

Looking ahead, the outlook for the future of data confidentiality in GIS is one where restrictions will likely tighten further as technology advances. Though cloud computing and artificial intelligence may provide powerful new methods for data analysis, they do so at some risk to privacy. As these technologies progress, there will be continuing needs for global standards to regularize how GIS data is both shared and protected.

Considerations or Implications of the Technology's Use

While GIS has many advantages, including better decision-making in fields such as urban planning and emergency response, its use also brings up ethical issues concerning privacy. Among the most serious concerns is the re-identification of geospatial data, especially when it is integrated with other publicly available information. Even anonymized data can sometimes be re-identified through advanced techniques, which undermines privacy protection.

Another issue that arises is surveillance and the potential misuse of data with the increased utilization of GIS in sensitive areas like public health and law enforcement. For instance, if tracking the movement of individuals is not appropriately done, it could easily lead to violations of civil liberties. Besides, ethical questions regarding ownership and control over geospatial data

also arise. This would be who owns the data, and how can individuals ensure their privacy is respected when their location information is used for public or commercial purposes.

In my opinion, even though the benefits of GIS are definitely there, there needs to be some more attention placed on developing ethical guidelines and technical solutions that protect individual privacy. It is very important that legislators and professionals in the field of GIS work together to develop systems that balance the need for data with the protection of civil rights.

Conclusion

In summary, GIS data confidentiality is an increasingly critical issue that will attain more relevance as the trend in using geospatial data soars. As GIS comes to be applied in health, public safety, and urban planning, just to name a few fields, it becomes of greater concern to guarantee protection for sensitive information from both personal and place-based perspectives. While technologies like GPS, mobile devices, and real-time data collection provide powerful tools to better decision-making and services, they also create significant risks with regard to privacy. Unless adequately protected, personal data gathered through GIS can be exposed or used inappropriately, leading to breaches of confidentiality and trust.

Over the years, a lot of effort has been made over the years with regard to those concerns. The establishment of guidelines laid down by different institutions, such as the Washington State Department of Social and Health Services, has been quite instrumental in ensuring the protection of confidentiality in geospatial data. Such initiatives, coupled with technological development in

encryption and other data anonymization techniques, are also contributing greatly toward security. Furthermore, international regulations on personal data handling, such as the GDPR, ensure a clear legal framework that not only allows for better organizational protection but also strengthens the protection of the individual.

However, in reality, with the continuous evolution in this field, there remain challenges in ensuring data confidentiality. The increasing complexity of applications, cloud computing, and the rise of artificial intelligence in geospatial analysis have given way to new opportunities for breaches in privacy. These advances need to be matched with strength in safeguards and updated legal frameworks. Going forward, policy thinkers, professionals in the art of GIS, and technology developers need to work together to establish appropriate standards that balance the social benefits of GIS with a respect for individual rights.

Ultimately, the future of GIS will rest on ongoing ethical guideline development and technological solutions that respect privacy concerns. By securing geospatial data, we can use this information to enhance lives and communities without threatening personal privacy and trust. The considered thought of these issues now will lay the groundwork for responsible and ethical use in the years to come.

Resources

Sharkova, I., Zerbe, J., & Stone, H. (n.d.). *Geospatial Data Confidentiality Guidelines*. Retrieved December 12, 2024, from https://www.dshs.wa.gov/sites/default/files/rda/reports/DSHS%20Geospatial%20Data%20Confidentiality%20Guidelines%20-%2004May2015.pdf

Kounadi, O., & Leitner, M. (2014). Why Does Geoprivacy Matter? The Scientific Publication of Confidential Data Presented on Maps. *Journal of Empirical Research on Human Research Ethics*, *9*(4), 34–45. https://doi.org/10.1177/1556264614544103

Rushton, G. (2007). *Privacy and Confidentiality in Health GIS*. https://proceedings.esri.com/library/userconf/health07/docs/closing/rushton.pdf

Curtis, A., Mills, J. W., Agustin, L., & Cockburn, M. (2011). Confidentiality risks in fine scale aggregations of health data. *Computers, Environment and Urban Systems*, *35*(1), 57–64. https://doi.org/10.1016/j.compenvurbsys.2010.08.002

Sherman, J. E., & Fetters, T. L. (2007). Confidentiality Concerns with Mapping Survey Data in Reproductive Health Research. *Studies in Family Planning*, *38*(4), 309–321. https://doi.org/10.1111/j.1728-4465.2007.00143.x