

GIS and Privacy

Stephen A. Matthews

Introduction

Surprisingly little is written about privacy and confidentiality issues in GIS texts - even "the GIS Bibles", and it would not be an error to suggest that the literature tends to be "grey". More specifically what literature exists tends to focus on the technological possibilities of geocoding rather than on concerns over privacy. Discussions of law and GIS tends to focus on litigation issues associated with "bad GIS" rather than a concern over violating someone's privacy with the release of identifying data. The status of legal protection for geospatial databases in particular differs in different countries and is constantly in a state of flux. The law impinges on the collection, dissemination, description, condition of sale, protection and liability aspects of geospatial data. Rhind (1996) identifies different types of laws that influence the "marketing of information." These are: public access laws (e.g., Freedom of Information Acts); human rights laws; fair-trading/anti-trust laws; copyright and intellectual property laws; data protection laws; public procurement laws; and, legal liability laws. For an extensive discussion see Onsrud (1995). If there is a message among some of the legal materials here it may well be that new technologies make old laws obsolete.

Following Wright (1997) privacy concerns are raised by GIS technology not only because some applications involve data about individuals but also because it can create a powerful new identifier - location. The concern is that location can become a personal identifier because GIS technology enables the synthesis and analysis of information not possible with other information management systems. On the one hand it has been argued that geospatial information should not raise privacy concerns because it is "factual" information about the land and resources, and therefore, by definition is not about identifiable people. On the other hand, the strong data integration and analysis capabilities of GIS, combined with the fact that most geospatial data are inherently local in nature, means that the technology has the potential to be far more privacy invasive than many other forms of technology (Onsrud, Johnson & Lopez, 1994). A related concern is that the analytical abilities of GIS will create the opportunity for information to be collected for one purpose and then used for unauthorized purposes or for users to be faced with the temptation to use information regardless of whether it is absolutely necessary or relevant to the task at hand (Wright, 1997).

As noted above, confidentiality and privacy concerns are almost invisible in the GIS literature, even the applied GIS literature (there are notable texts on the social aspects of GIS - see Pickles, 1995). The creator of information should be careful not to produce data sets that will be used "against" individuals or groups. In the case of GIS there is potential for abuse and for it to become a technology of surveillance and control. Curry (1996, 1997, 1998, 1999) and Goss (1994) observe that increasingly with technological developments everything is open to view and that geocoding more and more information will lead to a world without privacy - or a radically different form of privacy.

It is likely that the increasingly finer resolution and availability of geocoded data and their linking to survey data will fuel public concerns about invasion of privacy. We may unwittingly undercut the right to privacy. Also some geospatial information may have military significance, and almost all of it will have political significance. We therefore must act responsibly. In essence, we must maintain individual respondent confidentiality by aggregating up to a level where individual identity cannot be revealed. Furthermore, we must dispel rumors that confidentiality is not being maintained or that data will be used inappropriately.

GIA Core and Privacy

Following Monmonier (2002, p. 1) we note “the maps one looks at are less important than the spatial data systems that store and integrate facts about where we live and work.” In dealing with “the maps one looks at” we routinely employ several mapping strategies to avoid the most obvious privacy violations (Cromley and McLafferty, 2002). Strategies include, but are not limited to: turning geospatial data layers off (such as road network data so as to avoid providing location clues), displaying data on small-scale maps, aggregating data, and masking techniques. Regarding “spatial data systems” the data from projects used in a GIS environment are housed in restricted data directories within a Karlbridge firewall protected computer network within the Social Science Research Institute at Penn State. Users of these data are required to have completed the University Institutional Review Board human subjects training.

References

- Cromley, E.K. and S.L. McLafferty. 2002. GIS and Public Health Guilford Press: New York, NY.
- Curry, M.R. 1996. Data protection and intellectual property: information systems and the Americanization of the New Europe. Environment and Planning A 28, 891-908.
- Curry, M.R. 1997. The Digital Individual and the Private Realm. Annals of the Association of American Geographers 87, 681-699.
- Curry, M.R. 1998. Digital Places: Living with Geographic Technologies. Routledge: New York, NY.
- Curry, M.R. 1999. Rethinking privacy in a geocoded world. Chapter 55 in Geographical Information Systems (Volume 2) P.A. Longley, M.F. Goodchild, D.J. Maguire and D.W. Rhind [Eds.]. Wiley: New York.
- Goss, J. 1994. "We know who you are and we know where you live": the instrumental rationality of geodemographic systems. Economic Geography 10, 171-198.
- Monmonier, M. 2002. Spying with Maps: Surveillance Technologies and the Future of Privacy. University of Chicago Press: Chicago, IL.
- Pickles, J. 1995. Ground Truth: The Social Implications of Geographic Information Systems. Guilford Press: New York, NY.
- Onsrud H.J. 1995. Proceedings of the Conference on Law and Information Policy for Spatial Databases. NCGIA: Orono, Maine.
- Onsrud, H.J., J.P. Johnson and X. Lopez. 1994. Protecting personal privacy in using GIS. Photogrammetric Engineering and Remote Sensing 60 (9), 1083-1095.
- Rhind, D.W. 1996. Economic, legal and public policy issues influencing the creation, accessibility, and use of GIS databases. Transactions in GIS 1 (1): 3-12.
- Wright, T. 1997. Geographic Information Systems. Information and Privacy Commissioner/Ontario (also available at [http://www.ipc.on.ca/scripts/index .asp?action=31&P_ID=11405&N_ID=1&PT_ID=11351&U_ID=0](http://www.ipc.on.ca/scripts/index.asp?action=31&P_ID=11405&N_ID=1&PT_ID=11351&U_ID=0))