THE ROLE OF PUBLIC HEALTH POLICY IN THE DESIGN OF WEB MAPPING SERVICES

Rex G. Cammack
Assistant Professor
University of Nebraska Omaha
6001 Dodge St
Omaha, NE 68182
rcammack@unomaha.edu

Abstract

In the United States of America there is a national policy conflict between the freedom of information and the right to privacy. The perspective of this issue can be summarized as follows. The citizens of the United States pay with their tax dollars for all work done by the government so the result of that work is free to the paying citizens. The freedom of information policy in turn means that any information gathered by the government must be made available to its citizens. The opposing United States policy is the right to privacy policy. The general meaning of this policy is that information about individuals cannot be used for purposes other than for the one it was given. A good example of this policy is the 99-year limit on United States census information. The United States guarantees the answers that an individual gives will remain private for 99 years. The guarantee of privacy supersedes the freedom of information policy. This policy conflict has become more extreme in the digital data age because of the easy access to digital records instead of paper form. The United States government has strengthened its privacy policy in recent years in the area of public health information. The United States government is keenly aware that individual health records can easily be used to discriminate against an individual so it passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Prior to this act, health records could be exchanged more easily and used for purposes other than what they were given for.

A by-product of this policy change has led to a new cartographic technique called geomasking. Geomasking is the process of blurring the actual spatial pattern of geographic phenomena to disassociate the information shown with the actual person it is about. The process is a natural extension of the right to privacy concept. In the example of the United States census, all census data is aggregated into census aggregation units like blocks, block groups, counties and states. In the case of extremely low population density areas, the census will place data into adjoining units and label the actual unit with D in its table. D stands for nondisclosure. Most geomasking techniques have been developed for health data and focus on static maps in both the printed and World Wide Web (WWW) medias. The focus of this research is to look at the nature of the WWW, how geomasking is done, and how open web mapping

service providers can structure their services to insure geomasking is done appropriately by the users of these services. Evaluating both the technical approaches of web mapping services and theoretical cartographic concepts derived the study results.
The result of this research shows that a solution to the geomasking issue can be solved from a purely technology approach, a content theoretical approach or by a combination of both. The technology approach to solving the issue comes into forms access denial and scale dependent services. From the theoretical perspective, issues of generalization aggregation symbolization and select can all provide a method of successfully hiding the identity of individuals in the mapping process.

From these results one can surmise that web mapping services can be controlled to allow open access without violating the privacy policy and also meeting the policy of freedom of information.

Introduction

With large Internet Information Services (IS) available to the government and private individuals, the ability to map information has never been easier and more widespread. In this free cartographic space, the ability to translate vast amounts of data into spatial representations has led to a new concern about the privacy of individuals. The merit of this issue is well understood by many people for many different reasons. In its simplest form, individuals have the right to disclose information about themselves and when they disclose this information to the government. The government has the responsibility to not disclose that information to others (US Law Privacy Act 1974). Yet in countries such as the United States of America, the government is "by and for the people." The meaning of this can be interpreted as the people have possession of the government and have the right to access it. This concept is embodied in the Freedom of Information Act (FOIA) (US Law 1966). With the concepts of privacy and FOIA, there exists a balancing point that both proposed laws and the courts are trying to determine.

The goal of this research is to examine the conflicting intents of privacy and FOIA. By examining this issue from a cartographic perspective, some aspects of the cartographic process can be used to ensure adherence to the two issues. The result of this work can aid cartographers in designing and distributing information that provides both, individual privacy and also access to information.
For the purposes of this research, the focus on this topic is United State of America laws and policies. Most countries are endeavoring to deal with these issues in there own way but an individual countries situation and results can aid in the mapping process.

Background

For context purposes, three issues need to be explained in more detail to understand the focus of this research. This discussion is meant to give the reader a frame of reference and is not meant to be a complete legal analysis of government policy and laws. That

type of analysis is outside the scope of this paper, but many of the references provide a more detailed review of the issues.

Right to Privacy

Most American citizens believe there is an explicit right to privacy in the United States of America Constitution (U.S. Constitution), but that belief is not explicitly stated in the original document or its amendments. The issue of privacy has been the center of numerous legal debates and court cases (Rubenfeld 1989). The concept of privacy is implied in several amendments to the constitution. No single amendment addresses this issue directly but the implications of privacy exist in piecemeal form throughout these documents. The legal debate over privacy is long and complex, but this basic issue is where is the line between the governments control of ones life and where self-determination begins. The location of that line has moved throughout the history of the US. Constitution.

To provide some clarification for the government, the Privacy Act was passed in 1974 (The Privacy Act of 1974, 5 U.S.C. § 552a). The intent of this act was to set out guidelines on how and what information the federal government could release to other individuals without infringing on the disclosers privacy. Since the Privacy Act was passed, the US government has amended and created other new laws to control disclosure in one context or another. The two most germane to this research are: Family Education Rights and Privacy Act 1974 (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The first of these two acts provides delineation for what information US schools can disclose without consent of the student. Schools are required hold private much of the information held about students and are subject to disclose this information under information request. The HIPAA act deals with health information and its disclosure. Both of these acts are counterbalances to the Freedom of Information Act (FOIA).

Freedom of Information

Both FERPA and HIPAA are direct controls placed on the Freedom of Information request. These types of requests are made possible under the Freedom of Information Act (Freedom of Information Act 1966). Like Right to Privacy, the Freedom of Information concept is fluid in context to government pressures and policies. Numerous amendments to FOIA have been made based on government and legal actions. What holds true is that this right is commonly expressed as a natural right that has a longstanding presence in US law and only explicit exceptions to it are allowed.
Figure 1 illustrates conceptualization of how these different ideas interact, collide, and restrict one another. In the context of this research its important to note that maps and spatial data does fall within the gaze of these legal issues. One might find it interesting that maps are explicitly mentioned in the original FOIA. Maps about water wells were determined to be personal/private, so they were not to be disclosed.

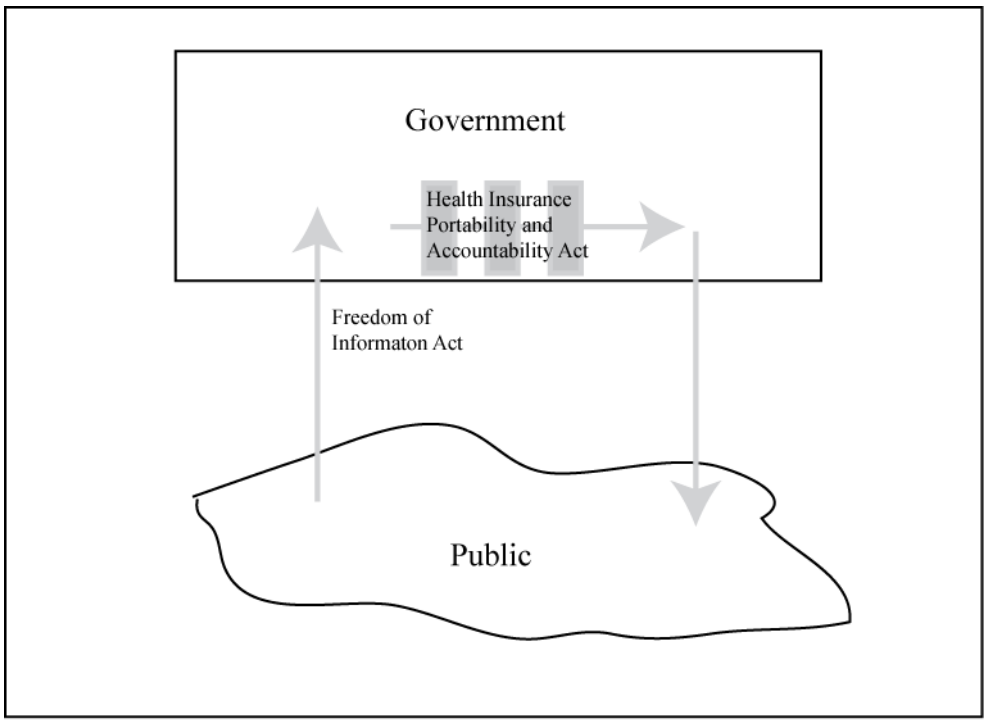

Figure 1. Public Access to Governmental Data

United States of American Census Bureau Disclosure

Geographers and demographers have dealt with disclosure issues over and over again in the context of counting the population of the United States (306,871,486) (U.S. Census Bureau 2009 July 9th). The process of collecting and distributing U.S. Census data has been changed for each decennial census. Distribution of data is controlled under Title 13, U.S.C., Section 9. The U.S Census Bureau stores copies of each returned census form, but there distribution is restricted until it is determined that the individual information no longer effects the provider. On April 1 of 2002 the 1930 census was opened to the public. The U.S. Census Bureau has determined, based on the life expectancy of people in 1930 being less than 60 years, that this information would no longer be restricted based on privacy issues (U.S. Census Bureau 2002).

In addition to the completed form, the U.S. Census Bureau has needed to examine its tabulated data before distribution to determine if it would disclose personal information. Once the data is collected and tabulated, it must pass through the U.S. Census Disclosure Review Board (U.S. Census Bureau 2001). This board applies a checklist to ensure that data does not violate Title 13, U.S.C., Section 9 for privacy. For tabulated data, private data is replaced with a "d" for disclosure rule and that data is then tabulated into other cells in order to protect its privacy. This practice allows access to information without private information being revealed. By examining this process, cartographers can begin to consider the methods for privacy in public health mapping.

Public Health Mapping

Richard et al. (1999) predicted that public health data in 10 years would be integrated and distributed effectively to speed critical analysis. Assessment of that prediction will be left to others, but it is clear that the issue of privacy has slowed that integration concept. With each data holding entity concerned about privacy, the exchange of data between trusted researchers is still not seamless and widespread. Yet the public is constantly seeking more openness in public health data. At the beginning of 2009 people from around the word became keenly aware of the HINI virus and its spread from a small Mexican town across the world. News media and private people were constantly mapping the spread of the virus and in some cases clearly identifying groups or individuals with the virus (see Niman 2009 http://flutracker.rhizalabs.com/). Government agencies in the U.S must comply with privacy rule making it hard for them to be open to the public.

The FluTracker is an excellent example of how Information Services (IS) can be integrated with Web Mapping Services (WMS). The spatial dimensions of public health data coupled with the timeliness and distributive power of IS/WMS derived maps provides a near boundless openness and transparency. So the societal goods of privacy and openness are in direct conflict. The simple analogy of this is what is good for me is not good for my neighbor. This opens the question of who gets to choose which is best for society. In the context of another common IS/WMS derived map service for sex offenders, the scale between privacy and openness is weighted much more to openness. The state of Oregon allows one to quickly locate the home address of individuals and map them (http://sexoffenders.oregon.gov/ July 9, 2009). The reason for this government openness is that the records and home addresses of sex offenders are explicitly open to the public under government laws and policies.

Privacy for Web Mapping Services

The issue at hand for cartographers is how do we create an IS/WMS system that allows full access to governmental spatial information under the idea of FOIA and protect the privacy of medical records embodied in HIPAA? The solution proposed in this research is good design. To bring home this point, cartographers must place design into a two-dimension aspect. Design must be divided into technical design (or system design) and theoretical map design. In the next section a more detailed look at both issues is given. Many of the ideas here are not new but it hoped that the end of this discussion that cartographic design framework will be seen to address this issue. It is clear that because many government and private groups holding public health data sets have their own rules based on their interpretation of HIPAA and privacy as a whole and that the IS/WMS solution will need to be custom fit to the need of each given group. Cartographic design of IS/WMS systems is client based so the client can filter data access before the cartographer gets a chance to formulate a map design. Or the client will dictate how the map image can appear.

Technical Design

When tasked with developing an IS/WMS of public health data, a set of technical specifications will need to be analyzed. The central method of data privacy control is access denial. One can trace this idea back to the FOIA where specific information was stated as off limits to the public. In this type of system, varying degrees of access denial must be set. Data users are divided into data managers, data users, and data viewers. Figure 2 shows how these three groups are further categorized into internal users and public users. The conceptualization of users and types of data used are critical to maintaining private data.

Manager Internal	User Internal	Viewer Internal
Manager External	User External	Viewer External

Figure 2. Technical Design - Authentication and Denial Model

IS/WMS systems have made it more difficult to maintain privacy in the context of spatial privacy. In the past, where large-scale geocoding of addresses was impossible or impractical, the control of privacy was inherent within the volume of data itself. With development of numerous public geocoding systems, the ease of taking that data and transforming into XML, RSS or KML, and dropping it on top of basemap mapping services like Google maps (2009), Yahoo maps (2009), or Bing maps (2009), restrictions by data volume is no longer a means of spatial privacy.

Theoretical Design

In the context of cartographic design theory, generalization is a principle concept used to control access to information and maintain privacy. The topic of generalization is extensive and complex and a discussion of the whole topic is beyond the scope of this paper. McMaster and Shea (1992) derived three components for generalization: why, when, and how to generalize. This simple conceptualization rights nicely into the issue of public health information mapping. The “why” question falls under the FOIA ideal. The public needs access to spatial information so they can make informed decisions regarding their health. On the other hand, the “when” question is controlled by HIPAA. Privacy is a right of the individual and people have the right to have health records kept private. So when a government organization needs to make public health information available, they will need to consider how to do this in the context of privacy. The consideration in this issue is “how to generalize” the information. McMaster and Monmonier (1989), McMaster (1989), and Solcum et al (2009) provides a generalization framework for both raster and vector data. The framework provides methods for dealing with data to make it private while still giving the public access to it.

Figure 3 shows how data can be generalized within the conceptual framework. The framework concept of aggregation is the most common method for maintaining privacy. By aggregating into spatial containers, the individualism of the person is lost. This method has been explicitly used by the U.S. Census Bureau to maintain privacy for census information. The only drawback to this method is that in low population density areas, having fewer neighbors increases the probability for an outsider to indentify individuals.

Another generalization methodology is displacement. Location shifting to hide the identity of a person is an effective method. In high population density areas, displacement can be done systematically such as moving the location of a health record to the nearest street intersection or in less populated areas moving the record to the center of a town or other geopolitical subdivision. The displacement will create a large enough uncertainty to keep information private.

A third framework concept is symbolization. In this context symbols can be exaggerated in size in relationship to the base map data to create ambiguity at the location of the health record. One needs to be careful with this approach in the IS/WMS approach and restrict this data to appropriate scales. A second consideration is to displace the data before hand. In a digital environment, it would be very easy for a user to derive a location and then remap the data to determine that exact location of the data.

The final generalization concept examined is dimensionally changing the data. Health data is private in a point data set. One can quickly change this point data into surface data (Rushton 1998). In geospatial analysis of health data, this approach is called spatial filtering. This approach is unsatisfying to map users since they know that the data is individually based and in their perspective the data should be point data.

Conclusions

From this research it has been identified that spatial information regarding health information is available under the FOIA in the United States, but HIPAA acts as a counter balance to FOIA in regards to the right to privacy. For organization wanting to map health information using an IS/WMS approach, some safeguards will need to be put in place. The research looks at these safeguards in the context of technical system design and cartographic design. The technical design may address issues of user categorization and authentication and service denial. Where as cartographic design issues are centered on the application of cartographic generalization and uses different aspects of generalization to the organizations advantage in order to provide more information to the public.

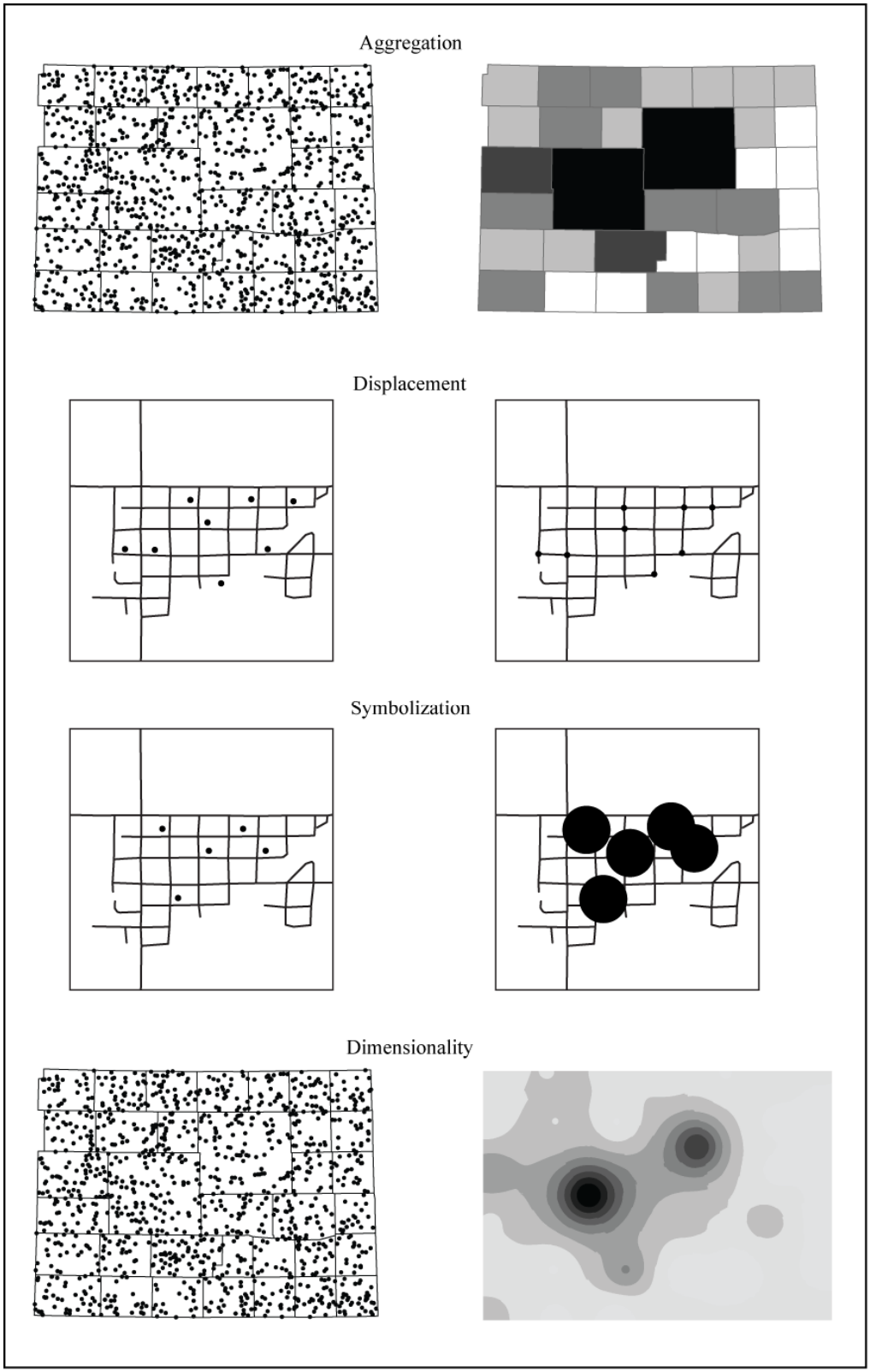

Figure 3. Generalization Frameworks Methods for Privacy

References

Google 2009. Google Map, http://maps.google.com/ accessed July 9, 2009

McMaster R. B. 1989. Introduction to Numerical Generalization. *Cartographica* 26(1) pp. 1-6.

McMaster, R. B., M. Monmonier 1989. A Conceptual Framework for Quantitative and Qualitative Raster-mode Generalization. *GIS/LIS '89 Proceeding* Vol(2) pp. 390-403.

McMaster, R. B., and K. S. Shea 1992. *Generalization in Digital Cartography*. Association of American Geographers Washington D.C.

Microsoft Corp 2009 Bing Maps. http://www.bing.com/maps/ accessed July 9, 2009

Niman, H. 2009. FluTracker. http://flutracker.rhizalabs.com/ accessed July 9, 2009

The Privacy Act of 1974, 5 U.S.C. § 552a

Richards, T. B., C. M. Croner, G. Rushton, C. K. Brown, and L. Folwer (1999) Geographic Information Systems and Public Health Mapping the Future. Public Health Reports: 114 pps 359-373.

Rubenfeld J. 1989. The Right of Privacy. *Harvard Law Review*, Vol. 102(4). pp. 737-807

Rushton, 1998. Improving the Geographic Basis of Health Surveillance using GIS. in G. Gatrell, A.C. and Löytönen, M. (eds) *GIS and Health*, Taylor and Francis, London.

Slocum, T. A., R. B. McMaster, F. C. Kessler, and H. H. Howard. 2009 Thematic Cartography and Geovisualization. Pearson Prentice Hall Upper Saddle River, NJ. USA

State of Oregon (2009). State of Oregon: Sex Offender Inquiry System. http://sexoffenders.oregon.gov/ July 9, 2009

U.S. Census Bureau. 2001. Disclosure Review Board www.census.gov/srd/sdc/wendy.drb.faq.pdf accessed July 9. 2009.

U.S. Census Bureau. 2002. National Archives Opens 1930 Census Records to the Public. CB02-CN.62

Yahoo! 2009. Yahoo! Maps, Driving Directions, and Traffic. http://maps.yahoo.com/ accessed July 9, 2009

§ U. S. Constitution.

§ U. S. Bill of Rights

§ Title 13, U.S.C., Section 9