INFORMATION PRIVACY AND THE USE OF GEOGRAPHIC INFORMATION SYSTEMS

Xavier R. Lopez and Harlan J. Onsrud
Department of Spatial Information Science and Engineering
National Center for Geographic Information and Analysis (NCGIA)
University of Maine
Orono, ME 04469-5711 USA

Abstract

This article examines current practices concerning the collection, maintenance, use and dissemination of spatially referenced information which may jeopardize the personal privacy of citizens. The application of geographic information systems (GIS) within government and industry are investigated and the impact of recent European Community data protection legislation on European and North American GIS activities is detailed. It also describes data protection rules and guidelines currently being proposed by various parties for adoption by the commercial sector and government. Special attention is given to the need to adopt harmonized data protection principles to guide both public and private sector spatial data handlers.

1 Introduction

Geographic information systems form part of the information infrastructure that is emerging throughout North America and Europe. The impact of the technology is immense, and places a heavy social responsibility burden on those involved with its application. The storage, display and analysis capabilities of Geographic Information Systems (GIS) software make highly effective tools for analyzing personal information. Geographic information systems also allow users to associate the graphic features in spatial datasets to attribute data such as address numbering to facilitate record matching. The strong data integration and analysis capabilities of GIS, along with the fact that much of the data in most GIS are inherently local in nature, gives the technology the tendency to be far more invasive of personal privacy than many other information technologies [1]. Without formal rules to guide this technology and related information handling activities, the potential for privacy invasion through inappropriate uses of personal information will increase.

Public entities collect, use, and disseminate a tremendous amount of personal information, much of it considered public data. For example, public utilities collect and maintain a variety of customer service information (e.g., phone logs, electricity use, sewerage discharge); local governments collect sensitive voting information as well as assessment information; the U.S. Census Bureau maintains confidential household data; hospitals maintains patient records which are geo-referenced to an address; and the local police maintain extensive databases on individual civil and criminal violations. Most of the personal information in these electronic databases have generally been collected to serve single purpose tasks necessary for improving the effectiveness and efficiency of our public institutions in providing public services.

However, as the ability to computer-match the large number records based on key values (e.g., name, address, social security, zip code, etc.) increases, the single purpose task can

become an enhanced one, thereby raising the threat of infringement of a person's informational privacy. As record-matching continues with little regulation, it is becoming increasingly necessary to confront the issue in all areas of government, including agencies using geographic information systems.

The distinction between inappropriate and appropriate uses of personal information is difficult to define and normative in nature, with diverse attitudes toward what is private information and how should it be used. Many individuals will not immediately see a threat to privacy in GIS, while others will feel threatened by record matching and similar capabilities. The following sections will address these issues in an effort to increase awareness of the importance of privacy considerations in public geographic information systems.

2 Privacy and Public Institutions

The concept of a right to privacy in the United States originated in an 1890 article by S.D. Warren and Louis Brandeis, 'The Right to Privacy', defining privacy as the 'right of an individual to be let alone' [2]. Many have since attempted to define or explain privacy, with some saying privacy is '..a value asserted by individuals against the demands of a curious and intrusive society' [3], or in other words is fundamental to the American conception of the proper balance of power between the people and their government. Since the time of Warren and Brandeis, protecting privacy from the encroachments brought by technological advancements has been a continuous tension.

Some government agencies, such as national statistical institutes (NSI), expend significant effort to ensure that he information leaving the organization is not individually identifiable. Maintaining confidentiality of individual records is an over-riding concern of the U.S. Census Bureau. The public's trust in the Bureau's confidentiality practices is essential to the success of each decennial Census [4]. However, it is doubtful that other public sector organizations practice the same level of data protection when dealing with personally identifiable records.

3 Tension Between Privacy Protection and Institutional Efficiency

The privacy right of the individual has always been a "compromise between two conflicting interests: his interest, on the one hand, to keep his own acts and circumstances to himself, and his interest, on the other hand, to reveal this information to others so that he may benefit from a more fruitful society". [5]. Balancing a public organization's information handling tasks with the privacy and confidentiality of those who have provided the data, is necessary to maintain the public's trust in government information collecting activities.

3.1 Efficiency in Government

Improving the efficiency of government operations has been a strong justification for introducing and maintaining detailed records of individuals. The use of computer databases has unquestionably increased agency efficiency and effectiveness in managing information resources. Maintaining cross-referenced data files on individuals is necessary in many instances for the equitable distribution of services and elimination of fraud and waste [6]. Likewise, health care providers need rapid access to a patient's past health records

(which may be recorded in various registers) to assess the proper diagnosis of an illness. For emergency response providers, the ability to instantly access a caller's phone number and address is essential to determine a rapid response.

Government agencies have clear interests in maintaining, complete, accurate information on individuals and property. Such information allows government to allocate scarce public resources equitably and efficiently. Moreover, cross-matching personal records with other datasets allows officials to identify fraud and waste by program beneficiaries. Government record keeping has benefited significantly from these computerized efforts. Some of the main benefits of computer matching are outlined below:

- Detection and Deterrence of Fraud, Waste and Abuse
- Improved Efficiency and Effectiveness in Government Programs
- Greater Public Confidence and Support
- Cost Effectiveness

Although the efficiency arguments in support of increased access can be persuasive, one must proceed with caution, particularly in balancing efficiency objectives with privacy goals [7]. To date, the major concern of database custodians has focused on the continued effectiveness of administrative functions and not in the protection of privacy [8]. The question now becomes, how far do we wish to allow government and other institutions to collect, use and disseminate information on individuals to pursue the goal of increased efficiency? This, of course, will be based on many factors including:

- public's awareness of government data collection, use and integrity.
- trust in government's ability to keep private information confidential.
- public's trust that their confidential information is not being abused.
- policy development which clearly distinguishes private from public data

3.2 Problems with Computer Matching

Invasive uses of personal information are possible in government, which has access to various public and commercial sources of personal information. Federal, state and local governments have the potential to provide a wealth of data such as census data, voting lists, remote sensing and photogrammetric images, land records, tax assessment, criminal histories, driving records, and car registrations, which could be cross matched in a GIS. It is important to note, however, that the sources mentioned are merely possible sources. Most legitimate uses of GIS would not require use of personal data, and national laws limit collection, use and dissemination of much of this information. While only a minority of government agencies would use GIS for invasive applications, fair information practices will remain voluntary for all agencies without clear public sector guidelines and enforcement mechanisms.

The repercussions resulting from even a perception of data misuse can be disastrous as the past Census cancellations in The Netherlands and West Germany attest. In the U.S. commercial sector, the Lotus Corp. dropped plans to market a CD-ROM with a complete listing of individual's credit information due to overwhelming public concern in 1988. These worries are heightened by the increasing flow of personal information across national boundaries and growing potential for satellite surveillance. As the creation and exchange

of spatial databases becomes global in scope, so too must data protection policies relating to their deployment, regulation and use.

The following problems with computer matching include:

- Lack of Government Oversight
- Cost
- Quality and Accuracy of Information
- Appropriate Use of Information
- Appropriate Use of Computer Matching and Profiling
- Merging of Regulatory Roles Concerning Information Handling

Without clear information dissemination policies which protect a citizen's privacy, public trust in government's handling of information may be compromised. This places some special responsibilities on data handlers to ensure the accuracy and security of the information. However, agencies should not wait for this issue to reach crisis levels before information privacy is addressed. Local authorities can prevent a public *backlash* by identifying potential privacy problems and administering clear information handling policies.

The manner in which government policies re-visit the privacy/access debate will have long-term repercussions as our public institutions undertake ever-increasing information-intensive activities. Unfortunately, it is highly unlikely that agencies will step up their data protection policies without considerable prodding. Moreover, deciding the "necessary" level of privacy is something that governments have very little inclination or ability to do for themselves [8].

4 Protecting Citizen's Right to Privacy

Maintaining individual privacy is a goal which should be considered from the onset of system implementation. Policy makers should fairly balance the efficiency advantages from these wonderful new technologies, along institutional and technical guidelines which will ensure compliance with privacy principles. In most cases, GIS technology is used and intended to benefit society. However, policy makers and GIS administrators must be vigilant to ensure that privacy is not abused through the use of these systems. Efficient government must be balanced with protecting citizen's right to privacy. Emphasis must be placed on information privacy enforcement, and in some cases, on the creation of clearer and stronger regulations and codes of practice which ensure a proper balance of these concerns. There are several steps that government GIS administrators and designers can take to promote sound information privacy protection. These can include:

- Establishing policies to guide privacy protection;
- Involving public participation
- Clear definition of sensitive data; and
- Stressing the of importance of privacy to staff; and
- Designing redaction capabilities as part of database software.

Such efforts are merely a few steps toward improving the protection of privacy within GIS applications in government.

5 Commercial Sector Activities

Public agencies are not the only organizations to benefit from the computerization of government records. The private sector, particularly real estate, credit agencies, banks and the target marketing professionals have a great interest in gaining access to personal records produced by government agencies. Such records include: Department of Motor Vehicles, Assessing, Voting Records etc.

While personal information use is a concern in government agencies, the commercial sector has been under less regulation than the public sector when collecting, using and selling individual information. The private sector regularly obtains public information from a variety of public and private sources including national statistical institutes, land registries, post offices, local government, lending bureaus, and other value-added data brokers.

The public's increasing unease over what personal information is being use and the manner in which it is being used has led to numerous calls to increase privacy protection both in North America and Europe [9]. A recent U.S. study estimates that during 1992 there were approximately one thousand bills in state legislatures aimed at restricting database management activities [10]. Although most of these piecemeal efforts were targeted at commercial database marketing activities, public tolerance of intrusions of privacy in both the public and commercial sectors is becoming short-fused. This increase in public awareness, and in some cases public hysteria, should be warnings to industry to review their information resource management activities [11]. Since a significant amount of data used by the information industry originates from government, public agencies must re-evaluate their indirect contribution to this problem [12].

It has been suggested that the commercial sector follow recommended government guidelines for data handling and that their general activities be, for the most part, self regulated [13]. Although self-regulation faces some difficulties in ensuring compliance, it has the benefit of allowing industry and government to work together in reaching a satisfactory solution. If, however, such a self-regulated alternative is ineffective, the alternative to enact tougher privacy protection on commercial database activities would be called for. This incremental approach is important in allowing the domestic information industries to move toward more open and responsible data handling policies.

6 Global Privacy Setting

Data protection can no longer be viewed from solely a national context. The transborder flow of personal information which is bundled with financial data and other types of information requires an international response [14]. However, one can expect national responses to these issues to have similarities and differences based on different levels of development, the political situation, and the legal setting. Despite national differences in culture, politics and institutions, there is strong pressure for nations to respond in similar ways. Why? The rapid evolution of a global information infrastructure (GII), coupled with the increasing transborder flow of data, requires greater international cooperation and convergence in policy responses. Table 1 outlines the status of OECD countries which have enacted data protection legislation and/or signed the Council of Europe Guidelines on data protection as of January 1993. This table highlights some of the national differences confronting efforts to overcome the barriers to the transborder flow of information.

Table 1: Status of Data Protection/Privacy Legislation in OECD Countries
(January 1993)

			Council of Europe Convention	
Country	*National*	*Sub-national*	*Signed*[1]	*Ratified*
Australia (Rev)	L*	L	x	x
Austria	CL		x	x
Belgium	L		x	x
Canada (Rev)	L			
Cyprus			x	
Denmark	L		x	x
Finland	L		x	x
France	L		x	x
Germany (Rev)	L	L	x	x
Greece	(P)			
Hong Kong	Z			
Hungary	L			
Iceland	L		x	x
Ireland	L		x	x
Israel	L			
Italy	(P)		x	
Japan	L*	L		
Luxembourg	L		x	x
Netherlands	CL		x	
New Zealand	L			
Norway	L		x	x
Portugal	L		x	
Spain	L		x	x
Sweden	CL		x	x
Switzerland	L	L	x	x
Turkey			x	
United Kingdom	L		x	x
United States	L	L		

Source: Transnational Data Communications Report, January 1993.

Code:

L	Law covers public/private sectors	(P)	Draft Legislation prepared
*	Public sector only	Rev	Law being revised
C	Constitutional Provision	Z	Guideline to be issued

[1] Signature Indicates intention to adopt domestic law and ratify the agreement.

We are currently witnessing the construction of such global systems in the development of global economic, trade, and telecommunications systems. These systems "collect, transmit, exchange and manipulate vast quantities of information, and overcome the traditional barriers to the international movement of information, time, language, distance, and cost" [15]. The transborder flow of various types of data will require similar global responses between trading nations to ensure the protection of personal data [16]. To do so will require *policy convergence* nations in response to the growing privacy problems.

6.1 European Community Responses

In its march toward a single European market, the European Community is harmonizing national laws which affect the development of the European economic market. One such proposal is the recently enacted directive to harmonize data protection legislation entitled "*Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* [17]. This Directive was approved in April 1995 after extensive amendment. The Directive recognizes that effective transborder flow of personal data now requires harmonized guidelines within European member states, as well as between trading nations. However, finding a common position has been difficult given the various national and cultural differences that influence the definition of privacy [18, 19].

The European Commission's amended proposal seems to have abandoned its initial strategy to establish a common policy which would comprise existing national regulations in European countries (i.e.. Germany's very strict privacy policy in contrast to the UK's which minimally complies with the Council of Europe Convention). Instead, the amended text has been simplified to omit differences in the treatment of the public and private sectors. Also, the amended proposal concentrates on processing of personal data, as opposed to hardcopy files. Furthermore, the Directive's approach has been to encourage codes of conduct at the national level. Codes can be applied to specific sectors (e.g., direct marketing, medical, law enforcement, education, etc.). Finally, the Commission held steadfast to the constitutional rights of individuals as the founding principles for the Directive. The impact of this Directive on European trading partners is uncertain. However, there have been some concerns, most notably in the United States over the scope of the Directive.

6.2 US Responses to the European Data Protection Directive

There has been much discussion in the United States regarding the growing issue of information privacy in general and the European Directive in particular [13]. The US data providers have a stake in the European proposal because of its extensive trade with the European Community and also because many observers believe that the privacy laws of the United States do not provide the level of protection that the Data Protection Directive requires--particularly concerning private sector information handling activities [ibid.]. Others are concerned that such restrictions could impair database marketing activities -- an industry well represented by U.S. firms [20, 21].

It is nearly inevitable that the U.S. become party to international data protection measures by adhering to the 1995 Directive. It is interesting to note that European Data Protection Directives originating outside American borders will likely bring about significant changes

to the manner in which the United State government and the private sector handle personal information. The challenge now facing public and private sector handlers of personal information is to adopt acceptable codes of practice which will ensure the information privacy of the public without undermining benefits to the organization brought about by using information technologies.

7 Conclusion

The controversy surrounding the government's role in eroding information privacy is growing. Public awareness of the privacy problem in Europe and North America has heightened with the increasing use of computing technology, the pervasiveness of digitized personal data histories, and the overall movement to conduct business transactions over electronic networks. The ultimate challenge to public and private information handlers will be to "create and foster an informed trust between the individual and state with respect to the collection and use of personal information [8]. Only then will our public institutions and commercial enterprises begin to renew the public's trust.

8 Acknowledgments

This work is based upon work partially supported by the National Center for Geographic Information and Analysis (NCGIA) under NSF grant No. SES-8810917. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

9 References

[1] *Rubin, Michael Rogers, 1988.* Private rights, public wrongs: the computer and personal privacy. Norwood, NJ: Ablex Publishing Corporation.

[2] Warren, S.D., and L. Brandeis, 1890. "The Right to Privacy." Harvard Law Review 4.5: 193-220.

[3] Post, R.C., 1989. "The Social Foundations of Privacy: Community and Self in the Common Law Tort." California Law Review 77.5: 957-1010.

[4] Nelson, Dawn D., 1987. "Record Linkage v. Confidentiality from the Perspective of the U.S. Bureau of the Census," Protecting Privacy, Automatic Data Processing and Progress in Statistical Documentation. Eurostat: Statistical Office of the European Communities. (Brussels, Office of Official Publications of the European Communities, 1987): 325-336.

[5] Organisation for Economic Cooperation and Development, 1980. OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Data. (Paris, OECD).

[6] Kusserow, Richard F., 1984. "The Government Needs Computer Matching to Root out Waste and Fraud." Communications of the ACM 27.6: 542-545.

[7] Lopez, Xavier, 1994. Balancing Information Privacy with Efficiency and Open Access. Government Information Quarterly. 11.3: in press.

[8] Flaherty, David H., 1989. Protecting Privacy in Surveillance Societies. Chapel Hill and London: The University of North Carolina Press. 467.

[9] Bennett, C., 1992. Regulating Privacy: Data Protection and Public Policy in Europe and the United States, Cornell University Press. Ithaca.

[10] Direct Marketing Association, 1992. 1991-1992 Compendium of Government Issues Affecting Direct Marketing. New York: Direct Marketing Association as reported in Cespedes, F.V. and H. J. Smith (1993): 10.

[11] Cespedes, F.V. and H. J., Smith, 1993. "Database Marketing: New Rules for Policy and Practice," Sloan Management Review. MIT Press, 34:4 (Summer 1993): 7-22.

[12] Potvin, Louise, 1991. "Privacy Issues in the Information Age: What Corporations Need to Know." Government Information Quarterly 8.1: 95-99.

[13] Onsrud, Harlan; Johnson, Jeffrey; and Lopez, Xavier, 1994. "Protecting Personal Privacy in Using Geographic Information Systems," Photogrammetric Engineering and Remote Sensing. (September 1994). Bethesda: PE&RS: 1083-1095.

[14] Kirby, Michael, 1991. "Legal Aspects of Transborder Data Flows, Computer/Law Journal 11.2: 233.

[15] Ragin, Priscilla M., 1993. "The Globalization of Privacy: Implications of Recent Changes in Europe," The American Journal of Economics and Sociology. July 1993. 52.3: 257-274.

[16] Reidenberg, J.R., 1992. "Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?" Federal Communications Law Journal 44.2: 195-243.

[17] Commission of the European Communities, 1995. Council Directive On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. COM (95) 422 final-SYN 287. April 13, 1995. Brussels.

[18] Rosenbaum, J.I., 1992. "The European Commission's Draft Directive on Data Protection." Jurimetrics Journal 33: 1-12.

[19] Raab, Charles, 1993. "Governance of Data Protection," Modern Governance: New Government Society Interactions. Sage Publications. 89-103.

[20] Schwartz, Paul, 1989. "The Computer in German and American Constitutional Law: Towards and American Right of Informational Self-Determination." The American Journal of Comparative Law. 27.4: 675-701.

[21] Trubow, G.B., 1992. "The European Harmonization of Data Protection Laws Threatens U.S. Participation in Trans Border Data Flow." Northwestern Journal of International Law and Business 13: 159-176.