

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

## **Protecting Personal Privacy in Using Geographic Information Systems**

Harlan J. Onsrud, Jeff P. Johnson and Xavier Lopez

Department of Spatial Information Science and Engineering &

National Center for Geographic Information & Analysis

### **ABSTRACT**

Personal privacy is a social issue of increasing relevance to the geographic information system (GIS) community. The power of GIS processing and the crossmatching of geographic datasets with other datasets are raising strong privacy concerns. This article discusses current practices and trends in the collection, maintenance, and dissemination of personal information by government and industry through the use of GIS and related technologies. It reviews the development of legal rights in privacy, discusses the societal importance of personal privacy, argues that self regulation of the use of personal information is a necessary goal for the GIS community, and describes privacy protection guidelines currently being proposed by various parties for adoption by the commercial sector and government. Finally, the article recommends specific privacy protection principles for adoption and self-imposition throughout the GIS community.

### **1. INTRODUCTION**

GIS forms part of the communications infrastructure that is emerging in the transition from an industrial to an information oriented society. Improved geographic information handling capabilities are continuing to find expanding applications throughout society and the eventual public and private investment in such capabilities is being estimated in many billions of dollars. Geographic information systems and their associated databases are substantially affecting the operation of government and business. The impact of the technology is immense, which places a heavy social responsibility burden on those involved with its promulgation. Along with its positive effects, the negative impacts of the technology and its associated databases need to be considered. The negative impacts need to be divulged, eliminated, minimized, or accommodated and weighed against the positive.

One of the potentially negative societal effects that GIS technology is helping to bring about is a decrease in personal privacy. From one perspective, geographic information has nothing to do with personal privacy - geographic information is factual information about land and resources. By definition it's not about individual people. However, from another perspective, geographic information systems are proving to be powerful data integrating technologies. Experiences of the marketing community indicate that the ability to integrate data by tying that data to its geographic location is one of the marketing industries most promising and powerful tools in compiling data from widely disparate sources on households and individuals - something that

was a practical impossibility a few short years ago (Eitenbichler 1993). The storage, display and analysis capabilities of GIS software make geographic information systems highly effective tools for analyzing personal information. Because of its strong data integration and analysis capabilities and because the data in most GIS are inherently local in nature, GIS technology has the potential to be far more invasive of personal privacy than many other information technologies.

Parties on both sides of the privacy debate generally agree that the expanding capabilities of technology and the increasing detail of information that is being incorporated into databases are combining to decrease the typical citizen's ability to keep their affairs private. Parties on both sides also seem to agree that most citizens are neither aware of the level of detail that is being collected on them nor of the extent that the information is being shared with others. Some advocates of the right to gather and trade in information on individuals have argued that the increased availability of personal information is merely returning society to the social scenario of small towns where everyone knew everyone else's business. The typical citizen is more than willing to give up some privacy in exchange for the substantial benefits that accrue from compiled databases. However, advocates of privacy protection point out that the entities that use personal information typically do so in an impersonal manner from distant locations. It is not a mutual relationship. Rather, it is government and commercial sector 'insider elites' that are compiling and using expansive knowledge about individuals' lives. Privacy advocates argue that, when asked, most people are unwilling to have personal information about themselves passed on to others for non-specific commercial or government purposes. The typical citizen is seldom asked for their opinion or approval and therefore has no opportunity to become informed or to object. Advocates of greater privacy protection argue that government and commercial sector insiders are making important decisions about the lives of individuals on the basis of information of which the individuals affected are often completely unaware.

As databases containing personal information come into more prevalent use, citizens are becoming more concerned about preserving their right to privacy. Several surveys have shown that citizen concern has steadily increased over recent years (Harris & Associates 1983; Privacy and 1984 1984; Smith 1990; Madsen 1992; Cespedes and Smith 1993). News articles addressing privacy issues are now frequent in national magazines and newspapers. The voicing of citizen concern over the privacy ramifications of proposed commercial and government actions have begun to increasingly alter or halt such actions. By example, Lotus Corporation was scheduled in 1991 to begin selling a marketing aid called "Marketplace" for use on desktop computers with data supplied on optical disks. Detailed information on the personal and shopping habits of approximately 80 million households (120 million Americans) would have been made accessible to virtually anyone with a computer (Reitman 1991). Although the search capabilities and provided databases would have been extremely valuable to small businesses, they also would have been valuable to those wishing to engage in burglary, fraud, sexual harassment, and a host of other illicit purposes. Lotus incurred a multi-million dollar loss when it dropped plans to make the software and data generally available two months before it was scheduled to go on sale and the company was subjected to extensive negative publicity (Miller 1991). One of the more visible examples in which privacy concerns have altered government actions is the cancellation of national censuses in the Netherlands and West Germany. Because these governments were unable to assuage or accommodate their citizens' concerns over privacy and the potential misuse of personal information, citizen resistance forced cancellation of the censuses and the many

substantial benefits of census taking were lost (Flaherty 1989). In light of strongly expressed citizens concerns, policy makers must reconsider how far to allow private industry and government to collect, manipulate and disseminate information.

There is no doubt that some uses of GIS datasets, although currently legal, would be considered by most citizens in the U.S. to be highly intrusive and controversial. Awareness and concern by citizens regarding such applications may lead to a legislative backlash. Backlash legislation tends to be overreaching and piecemeal. In attempting to address undesirable applications of GIS, such legislation may hinder many non-intrusive and socially desirable applications of GIS as well. Overreaching omnibus legislation would decrease the ability to provide services to consumers and would harm the long term development and use of GIS by government and industry. To avoid citizen overreaction and protect the investment in GIS databases, reasonable privacy policies need to be established and implemented by the GIS community. Members of the GIS community, in the interest of the public and in their own best interest, need a set of guidelines by which they can gauge their current and proposed actions in the use of personal information.

## 2. LEGAL RIGHTS IN PRIVACY

The ability to store and query large spatial databases is continuing to expand. Future advances in information technology, such as the National Information Infrastructure (NII) and multimedia telecommunications, are likely to further increase the availability of personal data. Yet the applicability of current privacy law within networked digital environments is far from clear.

### 2.1 Common Law

The legal right to privacy in the United States arose from a Harvard Law Review article written in 1890 by S. D. Warren and Louis Brandeis. Warren and Brandeis initially defined the right of privacy as the 'right of the individual to be let alone' and 'the right to one's personality' (Warren and Brandeis 1890). Over the years the judiciary has developed and clarified the right through case law. The right "prevents governmental interference in intimate personal ... activities and freedoms of the individual to make fundamental choices involving himself, his family, and his relationship with others" (*Industrial Foundation of the South v. Texas Indus. Acc. Bd.*, 679). The right protects individuals not only from intrusions by government but also from intrusions by other individuals. Invasion of privacy is a "... wrongful intrusion into one's private activities, in such a manner as to cause mental suffering, shame or humiliation to a person of ordinary sensibilities" (*Shorter v. Retail Credit Co.*, 330). Tort actions for invasion of privacy fall into four general classes: intrusion (e.g. eavesdropping or persistent unwanted telephone calls), public disclosure of embarrassing private facts (e.g. publicity of private information of a highly objectionable kind even though the information may be true), appropriation (e.g. appropriating your name or likeness for commercial gain), and false light in the public eye (*Prosser* 1960, 389). Within the second class, the constitutional right to privacy is limited primarily to "matters relating to marriage, procreation, contraception, family relationships, and child rearing and education" (*Paul v. Davis* 1976).

Although the word "privacy" does not appear in the U.S. Constitution, the U.S. Supreme Court over time has interpreted a right of privacy to exist for individuals under the First, Fourth, Fifth, Ninth and Fourteenth Amendments (Schwartz 1991). The right of individuals (or corporations) to withhold themselves and their property from public scrutiny, if they so desire, is supported in

equity by the courts in a proper case if there is no remedy at law (Federal Trade Commission v. American Tobacco Co.).

From the case law, it is plainly seen that the context within which common law privacy rights were originally argued and developed in the U.S. was one involving conflicts among singularly identified individuals. Although such law remains valid and provides some limited protection, we have entered a new social and technological era in which privacy conflicts involve detailed data collection and identity profiling on large portions of the population. Historically, where there is a statutory gap in regulating human behavior, the common-law mechanism of tort fills the gap. Yet, to date, judges have been loathe to expand privacy tort law to apply to the domain of detailed information gathering on all members of society (Dansby 1991). One may surmise that the judiciary believes, as a rule, that the legislative process is the preferred forum for determining whether, and to what extent, further rights should be carved out in protecting the information privacy of individuals.

## 2.2 Legislation

In addition to judge-made law, numerous legislative enactments address privacy in the U.S. at both the federal and state levels. The major federal privacy statute is the Privacy Act of 1974. The Privacy Act (1) allows individuals to determine what records pertaining to them are being collected, maintained, or used by federal agencies, (2) allows individuals to prevent records obtained for a particular purpose from being used or made available for another purpose without their consent, (3) allows individuals to gain access to such records, make copies of them and make corrections, (4) requires agencies to ensure that any record which identifies individuals is for a necessary and lawful purpose, and (5) requires agencies to provide adequate safeguards to prevent misuse of personal information (Privacy Act of 1974). However, critics argue that the provisions of the act have been poorly enforced and adhering to privacy protection guidelines has not been a priority for federal agencies (Flaherty 1989, 331).

Among additional U.S. federal acts addressing a range of privacy issues include the Freedom of Information Act, Fair Credit Reporting Act, Family Educational Rights and Privacy Act of 1974, Right to Financial Privacy Act of 1978, Electronic Fund Transfer Act, Privacy Protection for Rape Victims Act of 1978, Privacy Protection Act of 1980, Cable Communications Policy Act of 1984, Electronic Communications Privacy Act of 1986, Computer Matching and Privacy Protection Act of 1988, Video Privacy Protection Act of 1988, and the Telephone Consumer Protection Act of 1991. Each of these provides protection of privacy under specific circumstances. For instance, the Freedom of Information Act, limits the types of personal information that may be disseminated by federal agencies under FOIA requests. The privacy provision of this Act has been taken seriously by the courts and has occasionally been an effective deterrent to providing personal information to the private sector (McLean 1993). Additions and revisions to federal legislation relating to privacy issues have been numerous. Critics argue that the recent trend of amendments has been to weaken rather than strengthen federal privacy legislation in order to further the goals of the commercial sector and government agencies.

Many state governments in the U.S. have a general privacy act that mirrors the federal government's Privacy Act. These acts typically control the information that state agencies and local governments may gather on individuals. Also similar to the federal law situation, most

states have numerous separate acts addressing privacy problems in specific situations.

From a review of the federal and state laws, it is readily apparent that many of the existing acts address the limits of personal information that government may gather on private individuals. Most do not apply to the private sector. For instance, the Right to Financial Privacy Act relates to government access to the records of the banking, loan, and credit industries. The act provides that government may not have access to the information contained in the financial records of any customer of a financial institution except under certain restricted circumstances. The act does not address or limit the voluntary transfer of personal information among members of the banking, loan, and credit industries. Those acts that do address private sector use of personal data have been passed to-date primarily on a patch-work basis and are typically very limited in scope. Such legislation frequently passes only when questionable information handling practices are related to highly visible or newsworthy events. For instance, the Video Privacy Protection Act of 1988 was passed as a direct result of the newspaper publication of the video rental records of U.S. Supreme Court nominee Robert Bork (Doyle 1990).

A patch-work approach in passing privacy legislation is undesirable because it results in inconsistent treatment among different classes of information. For instance, personal privacy in video rental records is now protected by federal legislation whereas personal privacy in the groceries, magazines, medicines, and contraceptives that are run through the checkout scanner at your local grocery store is not. In addition, a legislative approach of carving out subsets of personal information to protect with separate laws may result in legislation that "appears" to address the problem comprehensively for that limited category but falls short of doing so. For instance, the Fair Credit Reporting Act states that personal data may be sold or transferred to those with a "legitimate business need for the information in connection with a business transaction involving the consumer" but the act fails to adequately define what is meant by "legitimate business need" or what actions constitute a "business transaction." Determination of the meaning of the terms is therefore left largely to the discretion of information sellers who have a vested interest in interpreting the terms as broadly as possible. In addition, a problem exists in that those intent on obtaining consumer information under false pretenses may be able to do so with minimal chance of detection (Rothfeder 1992). Even though the overall privacy protection benefits of the Fair Credit Reporting Act are substantial, the shortcomings of the Act illustrate that one may not assume that passing law after law covering additional categories of personal information is the most efficient or effective approach to protecting the information privacy of individuals.

Other federal statutes that address private sector use of personal data in isolated areas include the Cable Communications Policy Act of 1984, the Family Educational Rights and Privacy Act of 1974, and the Privacy Protection for Rape Victims Act of 1978. Each of these acts has an affect on the use of personal information in specific cases, but the overall effect of privacy legislation on the private sector is minimal due to the limited application of these laws. Thus, private sector use of personal information in the United States is largely unregulated, and at the discretion of private institutions.

### 3. CURRENT PRIVACY PROTECTION PRACTICES

Information privacy issues have regularly been publicized as unwarranted intrusions by information voyeurs peering into the personal files and lives of celebrities and politicians

(Warren and Brandeis 1890, Levinson 1988, Rothfelder 1992). However, the issue of information privacy is much broader and pervasive. Of greater concern is the systematic collection and maintenance of large volumes of personal data by government, commercial organizations, and other institutions. The tremendous cost of collecting and maintaining spatially referenced databases for large populations currently places such activities beyond the reach of the typical individual or small business. "Only large organizations (e.g., federal agencies, local government, credit reporting bureaus, database marketing firms) have the mandate or resources to collect and maintain large volumes of selected datasets for a significant population. As these organizations become more effective in their information handling activities, they will increasingly be able to produce information mosaics or profiles of households, property or individuals" (Lopez 1994). Concern over personal privacy is increasing as the public becomes more aware of the data that is being collected on them and the uses to which databases are being put without their previous knowledge or consent.

### 3.1 Government Practices

Government collects detailed records on individuals in order to accomplish its statutory mandates. As such, there are countless justifiable reasons for government to amass detailed information on individuals. It only makes sense that government agencies should increase their effectiveness and efficiency through the use of computerized databases. However, the potential for government abuse in the use of detailed databases of personal information and the rising instances of questionable use practices is leading consumers and public policy makers to question the adequacy of existing privacy protection laws and the ability of government agencies to effectively protect the personal information they have been allowed to collect.

In addition to legislation, administrative regulations are promulgated by agencies in accordance with controlling substantive and procedural law in order to provide direction for government administrators in protecting information privacy. Maintaining confidentiality while at the same time complying with open access policies requires the development of clear and consistent information handling policies. For example, the U.S. Census Bureau has, over the years, developed commendable policies aimed at ensuring individual confidentiality in its decennial census statistics (Nelson 1987, 327). This confidentiality has been maintained while providing meaningful small area statistics necessary for the provision of local government services. The Census Bureau also routinely rejects requests from other federal agencies to assist with computer matching activities (ibid. 327). These confidentiality policies have engendered a level of public trust that is critical to the success of future census counts. Unfortunately, such regulatory policies have not been nurtured and developed throughout all levels of federal, state, and local government.

Privacy protection is projected to erode at increased rates at local and state government levels in those instances where these governments are turning to the sale of local government data to recover the costs of GIS implementation and maintenance. Those local governments with experience in selling data to the private sector acknowledge that the data sets in greatest demand and generating the greatest economic return are those that relate to individuals or specific households. In a GIS context, reports indicate that cadastral data (i.e. the household level data that ties ownership information to the location and physical attributes of the land) has greater market demand than other GIS data files (Post and McLaughlin 1993, page). In a time of

decreasing budgets and programs to *reinvent government*, the sale of government data has become a politically popular means of generating revenue (Onsrud 1992a&b). When using a revenue generation approach as opposed to a marginal cost-recovery approach for the dissemination of government information, government has an economic incentive to sell information on private individuals with the greatest detail and in the greatest amount allowed. If the regulation of sale of personal information is not closely controlled through privacy laws and rigorously enforced, the sale of government information is likely to further involve the government's hand in decreasing individual privacy both directly and indirectly.

Realistically, it is highly unlikely that agencies at any government level will step up their data protection policies without considerable prodding. The government's need to be informed is in direct conflict with the individual's right to be let alone. This conflict means that government agencies have little incentive to establish strong privacy protection guidelines on their own because such guidelines inherently limit their ability to collect and handle personal information. Thus, determining the level of privacy protection required is something that governments have very little inclination or ability to do for themselves (Flaherty 1989, 13). In addressing the level of protection question, privacy scholars have argued that, as a matter of policy, public agencies should collect only that personal information that is necessary to carry out their organizational functions. Furthermore, personal information should only be used for the purposes it was intended and only after receiving express consent of the individuals who provided the information (Department of Health, Education and Welfare 1973). Both of these principles were incorporated into the U.S. federal Privacy Act, although the consent requirement has recently been weakened to a notice requirement under some circumstances involving computer matching activities accomplished by federal agencies (Computer Matching and Privacy Protection Act of 1988). Unless state legislation requires it, state and local government agencies are not bound to these privacy principles.

In those jurisdictions in which citizen consent is not required to use personal information for other purposes, the kinds of data handling practices that governments are likely to further pursue are illustrated by the current uses of computerized driver and vehicle registration systems. In some states, the Division of Motor Vehicles (DMV) has developed computerized driver and vehicle registration systems that are highly effective in tracking residents. The State of Wisconsin now has the ability to suspend people's driving privileges for not only refusing to pay traffic fines, but also for failure to pay library fees, shovel their sidewalk, or properly trim trees overhanging a neighboring property (Garfinke 1994, 87). In other states, DMVs are being used to undertake such activities as collecting owed back taxes, (California), discouraging dropping out of high school (Kentucky), and tracking down child support payments (New Jersey) (Ibid. 87). Lawmakers around the country have found that DMV tracking capabilities are so effective at controlling behavior that they have now begun looking for other ways to exercise this newfound power (Ibid. 127). Some state governments now have the ability to control individual behavior by threatening to revoke a driver's license for actions unrelated to driving.

The objective of tracking and correlating government information on individuals obviously serves some important and socially beneficial ends. However, the practice is troubling under the too often prevailing circumstance in which little incentive exists for government personnel to ensure the accuracy of the data that is being correlated from numerous sources. There also is typically little incentive for government personnel to encourage effective citizen access to

databases for the purpose of correcting or challenging data. Detailed government tracking of individuals is particularly disturbing in those jurisdictions in which increased numbers of state and local agencies are beginning to sell information resources to those in the private sector whose intent is to use the information obtained for non-government purposes.

### 3.2 Private and Commercial Sector Practices

Widespread integration of personal information by the commercial sector was impractical in the past because the information was contained in numerous disparate and distributed manual files. From both technical and economic perspectives, the building and networking of detailed databases on all members of a community, their property, and their habits is now a practical reality. Under current U.S. law, there is little to prevent those in the private sector with the resources to do so to cross match your name, address, height, and weight from your drivers license file (allowed in many states) with your scanned image (taken from any available photo identification card), cross match that with your ZIP+4 address location provided by the Census Bureau, cross match that with cadastral, taxation, and facilities records provided by local government, cross match that with the scanned bar-code purchases you make at grocery and other retail stores, cross match that with your social security number (which most of us have voluntarily released many times over to the commercial sector), and cross match that with any of the hundreds of other electronic databases that are being used daily to keep track of everything from magazine subscriptions to gasoline purchases. The practice of compiling all this information will become easier and more common with further development of networks and databases. Extensive crossmatching is already occurring and the practice is growing rapidly.

Detailed personal and household information has been compiled by the commercial sector for most economically active U.S. residents and households. Equifax, TRW, and Transunion are the big three credit reporting companies in the U.S. while Claritas and National Decision Systems are the most visible marketing companies with close ties to the credit reporting companies. By example, National Decision Systems keeps track of the following data categories on individuals and households: address, phone number, age, gender, ethnicity, religion, children's ages, smoking habits, veteran status, marital status, household income, dwelling type, buying habits, and lifestyle (Equifax and National Decision Systems 1993 and 1992 a-d). Such commercial files, with varying degrees of detail, are available on over 140 million Americans in approximately 100 million households (Equifax and National Decision Systems 1992 b-d). Typically, a buyer of information designates a combination of qualifying information in any or all of the information categories for one or more zip-code areas and receives a list of addresses meeting the criteria. Names corresponding to the addresses typically are not supplied by the major information service companies but are readily accessible in most instances by accessing either local or national phone directories available on CD ROM. At least one information company offers a GIS package that can integrate many of these types of information for direct marketing, retail location, and other purposes (Equifax and National Decision Systems 1993). Some of the personal data in these data sets is aggregated or inferred information; however, many of the major commercial data sets contain actual activity or behavior information on individuals that has frequently been verified from multiple sources.

Sorts by the national data service companies for a specific purpose appear to be reasonably priced and such information is gaining widespread use for numerous business and commercial

applications. It is prohibitively expensive at present to build your own detailed database for a community by purchasing the detailed data on individuals from one of the national commercial databases. However, it should be noted that many private businesses are now building their own marketing databases and, indeed, the fastest growing segment in the GIS industry in the U.S. is the commercial sector (GIS World 1993).

Within the commercial sector, personal information is being used in conjunction with geographic information systems for many applications in marketing, insurance, retailing, banking, real estate, utilities and other industries (Eitenbichler 1993). These applications are diverse and often very innovative. For example, one information company recommends an application where customers' license plate numbers can be recorded at the site of business, and later correlated with name, address, census tract and other information in a GIS (Melucci 1993). One can envision future applications, where cameras in drive-through establishments might scan license plate numbers of customers, and have personal files available before the customer receives service. Numerous additional commercial opportunities exist for using personal information in geographic information systems without the knowledge or consent of the individual.

### 3.3 International Perspectives

The increasing transborder flow of data will require harmonized guidelines between trading nations to ensure the protection of personal data while also providing support and favorable conditions for economic activity. The Organization for Economic Cooperation and Development (OECD), of which the U.S. is a member, has adopted principles aimed at protecting personal data among advanced industrial nations (Flaherty 1989, 11). The European Community is currently considering even stricter rules under a CEC Proposal on the Protection of Personal Data (Pearson 1991, Rosenbaum 1992, 5). The CEC proposal, however, illustrates the difficulty in reaching a common position among nations. The European member states differ in their views on personal privacy. Only six of the twelve nations currently have national data privacy laws and these vary in approach and scope. Some countries such as the United Kingdom, Portugal and The Netherlands have relatively liberal laws, while others like Germany have quite restrictive laws (Madsen 1992, 333-650). There are also cultural differences influencing the definition of privacy in each of the nations. However, it should be noted that the general trend in Western Europe is to be far more restrictive than current U.S. law.

Although the stricter Western European privacy laws have proven to be effective at maintaining high levels of privacy, the effects and advisability of similar regulations in the U.S. are uncertain. Privacy regulations inherently hinder, limit, or eliminate a range of economic activities. Some commentators have argued that the stringent requirements being proposed for international dealings will have severe effects in dampening current and future economic opportunities (Rosenbaum 1992, 9). There is a fear that restrictive European Data protection policies may place North American database marketing industries at a disadvantage. National laws or Community of European Communities (CEC) measures that restrict the transfer of national datasets to countries which do not maintain the same level of protection could impair the successful growth of U.S. database marketing activities abroad (Potvin 1991, 98). One counter argument is that much of the bias in dealing with U.S. firms will rapidly dissipate when U.S. law provides a comparable degree of information privacy protection in the commercial sector to that being proposed by the European Community (Trubow 1992).

#### 4. SOCIETAL IMPORTANCE OF PERSONAL PRIVACY

The importance of privacy has been the subject of much study in recent years (Post 1989; Wacks 1989; Trubow 1990; Rotenberg 1991 and 1993; Reidenberg 1992; Tuerkheimer 1993). Privacy advocates argue that personal privacy is essential to preserving constructive social and community interactions and will be critical to maintaining tenable democratic societies in a modern world (Post 1989). Some argue that social control through information systems is indeed a real threat and that extensive collection of personal data is likely to lead to a society that promotes homogeneity by discouraging actions that are perceived negatively by the majority. The rampant collection and use of personal information by government and commercial institutions substantially increases the likelihood of a "...conformist, robotic public seeking to avoid exposure to the risks inherent in functioning in society" (Trubow 1990). Detailed information gathering on all individuals in society by the commercial sector and government and the ability to quickly construct dossiers on individuals will have a 'chilling effect' on our willingness to deviate from the norm and on our willingness to question authority. The purpose of such compilations is to manipulate the individual, not to improve the ability of the data subject to act and decide (Simitis 1987, 733). Awareness that minute records of activities are being recorded is by itself probably enough to influence behavior and hinder the discourse of individuals (Ibid., 723). Social worth becomes increasingly measured by data profiles rather than through personal interactions and human dignity is lost. Diversity in opinions, perspectives, and experiences promotes innovative ideas and yet the productivity resulting from diversity decreases in a society in which detailed databases have the effect of decreasing risk taking by individuals. Over time, inability to control information about ourselves will make us passive citizens rather than active participants in society. Thus, in order to maintain viable democratic societies in a modern world, information privacy is the price that must be paid to secure the ability of citizens to communicate and participate (Ibid., 746).

The claim is made that the commercial sector in the U.S. already has "...become heavily intrusive, gathering and exchanging personal information about individuals without regard to the harm it may cause" (Graham 1987, 1395). Individuals that do not want their every purchase, movement, hobby, or political beliefs known already are being forced to resort to efforts to conceal their lives and beliefs. Privacy advocates further argue that those who lack the resources, knowledge, or will to conceal their private and financial lives will be coerced into a position of avoiding controversial or unpopular activities (Graham 1987, 1396) or, based on their unfavorable recorded profiles, will be excluded from sharing in certain economic and social benefits. Because government is increasingly able to purchase address lists and other personal data collected by the commercial sector, the boundaries between public and private collection of personal data have also become very blurred. Privacy advocates argue that democratic principles of governance will increasingly suffer as information surveillance becomes the order of the day and improper uses of personal information increase.

Those opposed to expanded privacy rights for individuals argue that the dangers of detailed databases are greatly exaggerated, far-fetched, and unlikely to effect the fabric of American democracy. The benefits to be gained through responsible use of databases containing detailed personal data far outstrip the largely subjective and non-quantifiable rights in personal privacy. Abuses in use should be controlled but not data collection itself. They further argue that it is far more beneficial for society to deal with privacy abuses on a case by case basis than to restrict

database building and the economic efficiency benefits deriving from expanded databases. Regardless of how the debate is eventually resolved concerning the best means of protecting information privacy, the underlying social reasons for protecting personal privacy are probably as valid today as they have ever been.

## 5. LEGISLATION AND SELF-REGULATION

The scope and effect of U.S. privacy protection laws are frequently criticized (Berman and Goldman 1989; Flaherty 1989; Trubow 1990; Rotenberg 1991; Madsen 1992). There have been many calls for new legislation that would actively require and enforce greater protection of personal privacy in both the public and private sectors. A recent study estimates that during 1992 there were approximately one thousand bills in state legislatures nationwide attempting to restrict database management activities (Direct Marketing Association 1992, 167). While most of these efforts target specific commercial database marketing activities, the public's intolerance of intrusive activities is increasing. This increase in public vigilance is a warning to both government and industry to reassess their information management activities.

The questionable acts of some businesses are inviting strict control of the entire information industry. By example, there are frequent calls for omnibus privacy legislation similar to the federal Privacy Act to apply generally to public agencies at all levels and to the private sector (Rubin 1988, 135; Flaherty 1989, 309; Rotenberg 1991). Typically one or more privacy commissions is envisioned as a means for enforcing the legislation and resolving privacy complaints (Trubow 1989; Reidenburg 1992, 242). Such legislation has been enacted in several European countries (Flaherty 1989; Madsen 1992) and the European Community has drafted a Data Protection Directive that would require such laws in all member countries. If applied to the commercial and government sectors in the U.S., this approach could potentially require all those managing geographic information systems containing any amount of personal data to be subjected to a series of bureaucratic processes and the administration requirements and authority of newly instituted privacy commissions. While privacy legislation would be targeted at preventing inappropriate uses of personal information, the bureaucracy of implementing and enforcing the law has the potential to place unnecessary burdens on legitimate uses of information in geographic information systems. Although political pressure is building to apply omnibus privacy regulation to the commercial sector, legislators should proceed cautiously. While such measures may provide a reasonable level of privacy protection, the costs to government and industry of the provision of public and private services would be markedly affected. Moreover, the impact of such a proposal on the competitiveness of the U.S. information industry is unclear.

Rotenberg argues that the right of privacy should be defined in a modern world as "the right of the individual to control the disclosure of personal information, and to hold those accountable who misuse information, breach a confidence, or who profit from the sale of information without first obtaining the consent of the individual" (Rotenberg 1991, 80). The consent requirement is a significant departure from current U.S. commercial practice and law. Although the requirement is being imposed in Western Europe, legislative attempts in the U.S. to limit the personal information that the commercial sector may collect have invariably been converted into requirements to ensure the accuracy of the data collected or to impose other conditions concerning the use of the information (Post 1989, 1009). The banning of private organizations

from collecting personal information without consent has never been imposed in the U.S. on a wide scale basis. The consent requirement, if applied to the commercial sector, would mean that data collected by one company could not be transferred to another company without the explicit consent of those individuals identified in the database by name, social security number, address or similar identifier. The requirement would significantly alter the means the commercial sector uses in cross matching datasets. One can envision an eventual commercial regime developing in which individuals set the price on their own privacy. For example, one might explicitly agree with an information clearinghouse to give up certain personal information in return for a small fee for each piece of "junk mail" received from businesses with whom one has never done business.

The foregoing comments raise the question whether new legislation needs to be written to redraw the legal line between "permissible exchanges of personal facts" versus "impermissible intrusions on privacy." Although the form they will take is yet unanswered, revisions to privacy laws in the U.S. are seen as essential by commentators on both sides of the privacy debate. Regardless of the form such laws eventually take, the GIS community should start implementing and gaining experience with sound privacy practices through an incremental process. The process should begin with the expedient development and adoption of appropriate privacy practice guidelines for the industry. The GIS community should not wait for privacy issues to reach crisis levels before taking action. If the industry is active in imposing reasonable information privacy practices on itself, eventual laws for controlling the detrimental effects of GIS on privacy are less likely to restrict the beneficial uses of GIS or will restrict them to a far lesser extent.

Self regulation is desirable because it is likely to result in an industry standard that is less restrictive and more adaptable to changing circumstances than a standard imposed by legislation or administrative rulings. Successful self regulation would demonstrate industry responsibility in addressing privacy concerns and would help ensure continuation of the social benefit image that geographic information systems currently enjoy.

The first step in creating an atmosphere of self regulation of the use of personal information in GIS is to develop guidelines or policies. As there are many professions and countries concerned about privacy protection, there are several sets of guidelines that may be consulted in the development of privacy guidelines for the GIS industry.

## 6. PRIVACY PROTECTION GUIDELINES

The more prominent information privacy protection guidelines include the U.S. Code of Fair Information Practices, the OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Data, the Association for Computing Machinery Code of Ethics and Professional Conduct, the Direct Marketing Association Guidelines, and the European Community Draft Council Directive on the Processing of Personal Data. These sets of guidelines have many similarities, but also important differences. Examination of these privacy protection guidelines can provide insights into the sort of guidelines that would be appropriate for use in conjunction with geographic information systems.

## 6.1 Code of Fair Information Practices

In 1973, the Code of Fair Information Practices was proposed for use in government automated data systems by the U.S. Department of Health, Education, and Welfare (HEW). The five privacy protection principles contained in those guidelines were:

- \* There must be no secret personal data recording systems;
- \* Individuals must have a means of learning about their stored personal information, and how it is used;
- \* Consent should be required for secondary uses;
- \* Individuals must have a means of correcting personal information; and
- \* Data controllers must maintain data and ensure data security.

(Department of Health, Education, and Welfare 1973)

While these guidelines were suggested in the dawn of the computer age, they were incorporated into the Privacy Act of 1974. The principles are still largely applicable to federal agencies today.

## 6.2 OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Data

The Organisation for Economic Cooperation and Development (OECD) is an organization consisting of 24 leading industrialized nations including the United States, Canada, Japan, Australia, and many European countries. In 1980 the OECD adopted a set of privacy guidelines. The guidelines were meant to apply to personal data in both the public and private sectors and were meant to be regarded as minimum standards capable of being supplemented by additional privacy protection measures in each member nation. The U.S. voted with the majority in recommending adherence to the guidelines and the OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Data are still frequently suggested as one of the most appropriate sets of principles for implementation and enforcement in the U.S. (Rotenberg 1993, 64; Madsen 1992, 195; Tuerkheimer 1993, 71). The OECD guidelines are composed of eight basic principles:

### \* Collection Limitation Principle

There should be limits to the collection of personal information. Collection should be lawful, fair, and with the knowledge and consent of the individual.

### \* Data Quality Principle

Data should be relevant, accurate, complete, and up-to-date.

### \* Purpose Specification Principle

The purpose of the information should be stated upon collection, and subsequent uses should be limited to those purposes.

### \* Use Limitation Principle

There should not be any secondary uses of personal information without the consent of the data subject or by the positive authorization of law.

\* Security Safeguards Principle

Personal data should be reasonably protected by the data collector.

\* Openness Principle

Developments, practices, and policies with respect to personal data should follow a general policy of openness.

\* Individual Participation Principle

Data subjects should be allowed to determine the existence of data files on themselves and be able to inspect and correct data

\* Accountability Principle

Data controllers, whether in the public or private sectors, should be held accountable for complying with the guidelines.

(Organisation for Economic Cooperation and Development 1980)

These principles are quite comprehensive and technology independent; they may be applied to the protection of privacy in geographic information systems as well as any other information technology. It should be noted that the OECD principles logically extend and expand those articulated by HEW in 1973. The fundamental principles for protecting personal privacy have not changed greatly from this time period. The most significant change appears to be increased calls for application of the fundamental principles to the private sector. Calls also have been issued advocating the application of similar privacy protection principles in developing the National Information Infrastructure (American Library Association 1993).

### 6.3 ACM Code of Ethics and Professional Conduct

Because of concern with use of personal information by the private sector, professional organizations have begun to also address the privacy issue. The Association of Computing Machinery (ACM) recently adopted a Code of Ethics and Professional Conduct for its members (Anderson et. al. 1992). A questionnaire requiring responses to a wide range of hypothetical ethical conflict scenarios was widely distributed among computer professionals (Parker, Swope and Baker 1990). Responses to the questionnaire and proposed provisions in the code were widely discussed at conferences and in the professional literature prior to passage. Although the code covers numerous topics, the provision on ethical conduct relative to protecting individual privacy now states that computing professionals should

...take precautions to ensure the accuracy of data ... protect it from unauthorized access ... allow individuals to review and correct their records.. (and) not use personal information gathered for a specific purpose for other purposes without consent of the individual (Anderson et. al. 1993).

These provisions are very closely related to the OECD guidelines. Most notably, secondary use

of personal information without consent is deemed unethical professional behavior.

#### 6.4 Marketing Community Guidelines

The Direct Marketing Association has also developed guidelines to advise its members of practice deemed acceptable by its membership. The provision relating to personal information states:

An individual shall have the right to request whether personal data about him/her appear on a direct marketer's files and receive a summary of the information within a reasonable time after a request is made. An individual has the right to challenge the accuracy of personal data relating to him/her. Personal data which are shown to be inaccurate should be corrected (DMA Guidelines, Article 4).

These marketing guidelines are far less stringent than the previous guideline examples because there is neither a requirement to notify data subjects nor a limit on secondary uses.

Cespedes and Smith argue that the marketing community in its own interest must go much further in protecting the privacy of individuals that are included in marketing databases. They are advocating wide scale adoption by the U.S. marketing community of the following general principles:

Rule 1: Data users must have the clear assent of the data subject to use personal data for database management purposes.

Rule 2: Companies are responsible for the accuracy of the data they use, and the data subjects should have the right to access, verify, and change information about themselves.

Rule 3: Categorizations should be based on actual behavior as well as the more traditional criteria of attitudes, lifestyles, and demographics.

They go on to state that Rule 1 includes the following corollaries:

Companies should avoid deception and secrecy in data collection.

Targeted consumers should know the marketer' source for information about them.

Individuals should have the opportunity to opt out of subsequent uses of data.

A consumer's assent to data use by one company does not automatically transfer to companies sharing that information (Cespedes and Smith 1993, 16.)

Once again we see expressed the same set of long articulated privacy principles although here they have been adapted to a specific information use domain.

#### 6.5 Information Industry Association (IIA) Fair Information Practices Guidelines

The Information Industry Association has adopted a set of fair information guidelines that consists of five general principles. Essentially, the principles encourage private companies to 1. establish a policy on fair information practices and monitor compliance with it, 2. protect personal information against unauthorized access, use, modification, disclosure or destruction

and ensure that others to whom personal information is transferred provide comparable protection, 3. disclose to data subjects the intended use of the personal information acquired from them or, if acquired from other than the data subject, use the information only for purposes consistent with the purposes of its initial acquisition, 4. maintain the highest level of information quality consistent with industry practice and customer needs, and 5. implement an inquiry and inspection procedure for data subjects (Information Policy Online.)

The IIA publishes their Fair Information Practices Guidelines along with a commentary and an eighteen point checklist in order to help companies to improve their information practices. Similar to the Marketing Community Guidelines, the burdens imposed in these guidelines in meeting informed consent and in protecting and correcting data are substantially less than the requirements recommended in most of the competing guidelines.

## 6.6 NII Working Group on Privacy

Currently the Working Group on Privacy of the interagency National Information Infrastructure (NII) Task Force is updating the privacy provisions of the previously discussed Code of Fair Information Practices. The working group recently circulated a draft of "Principles for Providing and Using Personal Information" (IITF Gopher/Bulletin Board). The goal of these principles, similar to that of the original Code of Fair Information Practices, is to provide a broad framework for addressing privacy issues that spans all sectors of the economy, including all public and private entities. It is hoped that legislators, regulators and companies will consult this basic set of responsibilities and relationships as they develop codes of practice to meet specialized circumstances. The proposed principles and accompanying commentary are much more specific than the previous Code of Fair Information Practices and have been framed to apply primarily in the context of data handling over the National Information Infrastructure. The current draft (June 1994) includes principles organized under the following headings:

### I. General Principles for the National Information Infrastructure

#### A. Information Privacy Principle

#### B. Information Integrity Principles

### II. Principle for Information Collectors (i.e. entities that collect personal information directly from the individual)

#### A. Collection Principle

### III. Principles for Information Users (i.e. Information Collectors and entities that obtain, process, send or store personal information)

#### A. Acquisition and Use Principles

#### B. Protection Principle

#### C. Education Principle

#### D. Fairness Principles

## IV. Principles for Individuals who Provide Personal Information

### A. Awareness Principles

### B. Redress Principles (IITF Gopher/Bulletin Board)

The principles go further in protecting personal privacy than those being recommended by the Information Industry Association or the marketing community. However, noticeably lacking in the principles is the requirement of explicit consent in the situation where personal information is transferred to a third party. Instead, a middle ground position is taken in which data collectors are required to inform individuals what they "expect" personal data to be used for and must provide the informed opportunity for individuals to limit data use if a subsequent intended data use is incompatible with the original purpose for which it was collected. The accompanying commentary goes on to explicitly point out that "...before incompatible uses occur, they must either be authorized by law or the individual data subject should be notified so that he or she can opt out of such use" (Ibid., paragraph 28). However, the interpretation of whether subsequent use is incompatible with the original purpose for which it was collected appears to be left primarily in the hands of the data user rather than in the data subject, from a practical perspective. The guidelines assume that, within the bounds of the "original purpose of collection", the secondary use of personal information and the transfer of personal data to third parties will be very common and should be expected by individuals providing personal data.

To avoid confusion, it should be noted that the National Telecommunications and Information Administration (NTIA), an agency of the federal executive branch, also is currently examining privacy issues. However, the focus of their study and proposed policy positions are focused specifically on the media and telecommunications industries.

### 6.7 European Community Draft Council Directive on the Processing of Personal Data

Finally, the GIS community should be aware of the information privacy principles being advocated and legislated in the international arena. In July 1990, in an attempt to address differences in the national privacy legislation among the nations of Europe, the European Community presented to the Council of Europe a draft directive concerning the protection of individuals in relation to the processing of personal data. The eventual goal is that all European nations will alter their national laws to conform to a common set of privacy principles. Consistency in laws is necessary in order to more readily transfer data among nations and to accomplish a unified European market.

Major sections included in the Directive include those addressing the lawfulness of processing personal data in the public sector, the lawfulness of processing personal data in the private sector, the rights of data subjects, data quality, provisions specifically relating to certain sectors, liability and sanctions, and the transfer of personal data to parties in third countries (Council of the European Communities 1990). Most germane to the present discussion are the general rights to be granted to data subjects in all nations adhering to the Directive. Article 14 states that all member nations of the European Community shall grant a data subject the following rights relative to processing of personal data in both the public and private sectors:

1. To oppose, for legitimate reasons, the processing of personal data relating to him.

2. Not to be subject to an administrative or private decision involving an assessment of his conduct which has as its sole basis the automatic processing of personal data defining his profile or personality.
3. To know of the existence of a file and to know its main purposes and the identity and habitual residence, headquarters or place of business of the controller of the file.
4. To obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in a file and communication to him of such data in an intelligible form. The Member States may provide that the right of access to medical data may be exercised only through a doctor.
5. To obtain, as the case may be, rectification, erasure or blocking of such data if they have processed in violation of the provisions of this Directive.
6. To obtain upon request and free of charge the erasure of data relating to him held in files used for market research or advertising purposes.
7. To obtain, in the event of the application of paragraph 5 and if the data have been communicated to third parties, notification to the latter of the rectification, erasure or blocking.
8. To have a judicial remedy if the rights guaranteed in this Article are infringed.

Article 12 ensures that any consent given by a data subject to use personal information is 'informed consent' and Article 13 specifies the minimum information that must be supplied to a data subject at the time personal data is collected from a subject.

The European Draft Council Directive is far from being final. The current draft has been rejected by the European Parliament and is currently undergoing revision (Bradgate 1994). The current draft has been severely criticized for going far beyond the level of protection necessary to head off likely incursions on personal privacy. The next draft is likely to be less stringent in protecting personal data but the degree to which it will be watered down is yet difficult to predict.

## 7. PRIVACY PROTECTION PRINCIPLES FOR THE GIS COMMUNITY

Specific to geographic databases, one might ponder whether large scale aerial photography, orthophotography, and high resolution remote sensing imagery raise privacy concerns and therefore should be subjected to some form of societal control. For instance, Dow Chemical v. United States, concerned aerial photography of a Dow Chemical facility where Dow claimed that the collection of high detail imagery over their site was an invasion of privacy and a violation of their Fourth Amendment rights. Although the District Court held that the aerial photography was a 'violation of Dow's reasonable expectation of privacy and an unreasonable search in violation of the Fourth Amendment', the U.S. Supreme Court held that the 'open field' doctrine applied to the case, and there was no invasion of privacy (Dow Chemical v. U.S., 1986). We contend that the finding in this case was appropriate and that there should be little legal control over the data that may be collected through conventional forms of aerial mapping and imaging systems, whether by government or the private sector.

It is personal attribute information extracted from aerial imagery that may infringe upon a

citizen's privacy rather than the imagery itself. Personal information extracted from aerial imagery would necessarily be subject to any guidelines proposed for regulating the uses of personal information in conjunction with geographic data handling. However, privacy guidelines should not extend into the realm of placing limits on imaging technology itself or placing limits on the scale of imagery that may be collected. To do so would be highly impractical and any privacy benefits likely to accrue would be far outweighed by the detrimental effects of not having such imagery available. Rather than resorting to guidelines or legislation that extend into this domain, use of geographic data that infringes on the existing privacy rights of individuals should be dealt with by the courts on a case by case basis.

In a sense, the general principles for the protection of informational privacy in the U.S. in the use of GIS have already been developed. The following list was developed by observing common threads in the privacy protection guidelines and laws that have already been recommended by others for the information industry generally. The principles are an attempt at a middle ground approach that considers not only the privacy needs of individuals but also the needs of government and commercial interests to have access to personal information. In the following guidelines, "personal data" means any information relating to an identified or identifiable individual or household.

Because the OECD Guidelines have already been agreed to in principle by the leading industrial nations of the world, those principles provide a rational basis upon which to base privacy guidelines for the GIS community. Following closely the language of those guidelines, we recommend adherence to the following fundamental principles in handling personal data in the GIS community:

\* Collection Limitation Principle

There should be limits in the types and extent of personal information collected for, contained within, or used in conjunction with geographic information systems. Collection should be lawful, fair, and with the knowledge and consent of the individual.

More specifically, no data identifiable to individuals or households should be collected or maintained in a GIS that relates to family matters, child rearing and education, marital matters, procreation, or contraception. Further, no data should be collected in a GIS on individuals or households if the exposure of the data, even if true, is likely to cause mental suffering, shame, or humiliation to a person of ordinary sensibilities or if exposure is likely to interfere with the ability of the data subjects to make fundamental choices involving themselves, their families, and their relationships with others.

Data on individuals or households regarding age, gender, ethnicity, religion, health, marital status, and consumer purchases are specifically allowed to be collected and processed in conjunction with the use of GIS, provided that such collection and processing do not otherwise breach the requirements of the preceding paragraph and are accomplished in strict accordance with the other provisions imposed by this code.

\* Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used. To the extent

necessary for those purposes, personal data contained within or used in conjunction with a geographic information system should be accurate, complete, and up-to-date.

This principle presupposes that the purposes of personal data use must be explicitly articulated prior to collection and that personal data is not to be collected for future unknown or speculative purposes. If personal data cannot be maintained as accurate, complete, and up-to-date, this principle requires that the personal data be expunged from the system.

\* Purpose Specification Principle

The purposes for collecting personal information should be stated upon collection. In most instances, this statement should be made directly to the data subject from whom the data is being collected. Subsequent uses of personal data should be limited to those purposes or to those purposes that are not incompatible with the original collection purposes.

\* Use Limitation Principle

Personal data should not be disclosed to others, made available to others, or used for purposes other than for which the data were collected without the explicit consent of the data subject or by the positive authorization of law. Consent to the transfer of personal data to others must be informed and the data subject should be allowed to withdraw consent at any time.

\* Security Safeguards Principle

Personal data should be reasonably protected by the data controller/administrator. Security safeguards should be provided by the GIS controller against such risks as unauthorized access, destruction, use incompatible with original collection, and unauthorized modification of data.

\* Openness Principle

Developments, practices, and policies with respect to personal data should follow a general policy of openness. Secrecy in collecting data and deception in obtaining consent must be avoided. The GIS controller should be able to readily determine the existence and nature of personal data contained in the system for any specific individual and the system should keep track of the sources from which data about individuals and households has been obtained.

\* Individual Participation Principle

Data subjects should be allowed to determine the existence of data files on themselves and be able to inspect and correct data at no cost or marginal cost. Upon request to the GIS administrator, data subjects should be provided with the sources from which data about them has been obtained.

\* Accountability Principle

GIS data controllers, whether in the public or private sectors, should be held accountable for complying with these guidelines.

We recommend that these fundamental principles be discussed, revised as necessary, and then formally incorporated into the professional codes of conduct of professionals and practitioners

affiliated with the GIS community. Other international, national, and commercial guidelines should additionally be referenced when working within a particular context, such as direct marketing.

The GIS industry should explore means for encouraging and extracting compliance with the guidelines. One means would be for professional organizations or industry groups to grant a "Good Data Handling Seal of Approval" to those businesses and government agencies complying with the privacy guidelines (analogous to the 'Good Housekeeping Seal' ) (Cespedes and Smith 1993, 20). Existence of the program should be widely advertised and promoted throughout the industry and to the public. Conversely, professional organizations and industry groups should "...publicize and ostracize bad practice" (Ibid., 20). Perhaps an award analogous to former Senator Proxmire's 'Golden Fleece Award' might be appropriate in cases where highly questionable business practices in violation of the code's provisions have caused substantial damage to the public's trust in the industry.

Adoption of the proposed guidelines would show a serious commitment by the GIS community to protect informational privacy. The GIS industry needs to ensure that geographic information technologies do not become part of the problem rather than part of the solution in addressing society's pressing social needs. Through self regulation of appropriate privacy practices, the GIS community can help ensure that GIS technologies and databases will continue to be perceived as socially desirable and beneficial.

## 8. SUMMARY

The vast collection, maintenance and dissemination of personal information by government and industry has increased public suspicion that their personal information privacy is eroding. Personal privacy is an issue that will continue to grow in importance as the potential for invasive information handling grows and the public becomes more aware of the threats to their personal privacy.

The privacy regulations of individual countries reflect national differences in culture, politics, and the expected roles of their institutions. However, as trade in information commodities becomes increasingly important internationally, the need for international data protection standards increases dramatically. It is important that the U.S. become a leader in shaping these standards. U.S. policy makers must craft a solution that effectively balances among the right to privacy, the right of citizens to access government information, and economic interests of the nation. Such a solution must provide information privacy for the American people without destroying the competitiveness of our information industries (Potvin 1991, 98).

Geographic information systems are contributing to the information privacy problems currently confronting society. Uncertainties in current privacy law in the U.S. and confusion over the appropriateness of various privacy protection practices are significant impediments to the development, sharing, and integration of geographic data sets. Although most GIS applications are viewed by the public as socially beneficial, many current and future applications may be considered as highly intrusive. '...Failure to reassure a skeptical public about the civil liberties implications of new information technologies may make it impossible to put promising technological solutions to work' (Flaherty 1989, 309). The GIS community has a substantial interest in maintaining citizen trust in geographic information technology. To maintain and earn

that trust, reasonable privacy policies need to be established and implemented in developing spatial databases and in networking them with other databases. Awareness by the GIS community of privacy protection issues will promote fair information practices generally and prepare the GIS community to have a voice in the drafting of future privacy legislation. Adoption and promotion of privacy protection guidelines such as those set forth in this article will contribute to the long term health and growth of the GIS industry.

## 9. ACKNOWLEDGMENTS

This work is based upon work partially supported by the National Center for Geographic Information and Analysis (NCGIA) under NSF grant No. SBR 88-10917. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

## 10. REFERENCES

American Library Association (1993). Principles for the Development of the National Information Infrastructure. Proceedings from the Telecommunications and Information Infrastructure Policy Forum. September 8-10. ALA, Washington D.C.

Anderson, R.E., G. Engel, D. Gotterbarn, G.C. Hertlein, A. Hoffman, B. Jawer, D.G. Johnson, D.K. Lidtke, J.C. Little, D. Martin, D.B. Parker, J.A. Perrolle, and R.S. Rosenburg, "ACM Code of Ethics and Professional Conduct," Communications of the ACM, May 1992, 33(5): 94-99.

Anderson, R.E., D.G. Johnson, D. Gotterbarn, and J. Perrolle, "Using the New ACM Code of Ethics in Decision Making," Communications of the ACM, Feb 1993, 36(2): 98-107.

Berman, J. , and J. Goldman (1989). A Federal Right of Information Privacy: The Need for Reform. Washington, D.C.: The Benton Foundation.

Bradgate, R. (1994). Privacy and Telecommunications, Working Paper. Sheffield, U.K.: University of Sheffield.

Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2779 (1984)

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

Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100-503, 102 Stat. 2507 (1988), Pub. L. No. 101-56, 103 Stat. 149 (1989), Pub. L. No. 101-508, 104 Stat. 1388-334 (1990)

Council of the European Communities (1990). Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data.

Dansby, H. Bishop (1991). Informational Privacy and GIS. Annual Conference of the URISA. San Francisco, CA: URISA. 4: 18-28.

Department of Health, Education and Welfare (1973). Records, Computers, and the Rights of Citizens. Washington D.C.: U.S. Government Printing Office as reported in Tuerkheimer, 1993.

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.

Dow Chemical v. U.S. (1986). 536 FSupp 1355 (EDMI 1982) rev'd 749 F2d 307, Aff'd 476 U.S. 227, 106 SCt 1819, 90 LEd 2d 226 (1986)

Doyle, Charles (1990). "Privacy in the Age of Computers." CRS Review. July/August: 6-8.

Eitenbichler, S.B., ed. (1993). GIS in Business '93 Conference Proceedings. Boston: GIS World, Inc.

Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986)

Electronic Fund Transfer Act, Pub. L. No. 95-630, 92 Stat. 3728 (1978), Pub. L. No. 97-375, 96 Stat. 1825 (1982), Pub. L. No. 101-73, 103 Stat. 440 (1989), Pub. L. No. 102-242, 105 Stat. 2301 (1991)

Equifax and National Decision Systems (1993). "InfoMark-GIS : Tomorrow's Technology for Today's Business Success". Atlanta: Equifax, Inc.

Equifax and National Decision Systems (1992a). "Introducing Direct Marketing Solutions". Atlanta: Equifax, Inc.

Equifax and National Decision Systems (1992b, c, d). "Polk Totalist File Rate Card"; "Metromail Rate Card"; "MicroSelects™ Database Rate Card". Atlanta: Equifax, Inc.

Fair Credit Reporting Act, Pub. L. No. 91-508, 84 Stat. 1128 (1970), Pub. L. No. 95-598, 92 Stat. 2676 (1978), Pub. L. No. 101-73, 103 Stat. 439 (1989), Pub. L. No. 102-242, 105 Stat. 2300 (1991), Pub. L. No. 102-537, 106 Stat. 3531 (1992), Pub. L. No. 102-550, 106 Stat. 4082 (1992)

Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, 88 Stat. 571 (1974)

Federal Trade Commission v. American Tobacco Co., 264 U.S. 298, 44 S.Ct. 336, 68 L.Ed. 696

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

Freedom of Information Act, Pub. L. No. 89-487, 80 Stat. 250 (1966), Pub. L. No. 90-23, 81 Stat. 54 (1967), Pub. L. No. 93-502, 88 Stat. 1561 (1974), Pub. L. No. 99-570, 100 Stat. 3204-48 (1986)

Garfinke, S.L., "Nobody Fucks with the DMV," Wired, 2.02 (February 1994): 87- 127

GIS World (1993). "Business Geographics Growth Leads GIS Market". Fort Collins, CO: GIS World, Inc. October. 11.

Gootee, Jane M. (1990). "Aerial Searches: A defendant's Perspective - Dow Chemical v. United States." Earth Observation Systems: Legal Considerations for the '90's. American Society for Photogrammetry and Remote Sensing, American Bar Association. Bethesda: 42-86.

Graham, Jonathan P. (1987). "Privacy, Computers, and the Commercial Dissemination of Personal Information." Texas Law Review June: 1395-1439.

Harris and Associates (1989) The Road After 1989: "A Nationwide Survey of the Public and its Leaders on the New Technology and Its consequences for American Life" as reported in Berman, J. and J. Goldman (1989).

IITF Gopher/Bulletin Board System: 202-501-1920, iitf.doc.gov (June 1994)

Industrial Foundation of the South v. Texas Indus. Acc. Bd., Tex., 540 S.W.2d 668, 679.

Information Policy Online. (iia.ipo@his.com) 1.2 (April 1994): item 3

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

Levinson, Sanford (1988). "Public Lives and the Limits to Privacy." Political Science and Politics. 21. 2: 263-280.

Lopez, Xavier (1994). Balancing Information Privacy with Efficiency and Open Access. Government Information Quarterly. 11.3: in press.

Madsen, Wayne (1992). Handbook of Personal Data Protection. New York: Stockton Press.

McLean, Decker (1993). "Privacy Gaining Heft as an FOIA Exemption." Communications and the Law 15.1: 25-46.

Melucci, John A. (1993). "Using License Plate Surveys to Define Retail Trade Patterns". GIS in Business '93. Boston:GIS World. 1:139-142

Miller, M.W. "Lotus Is Likely to Abandon Consumer Data Project." Wall Street Journal Jan 23, 1991, B1.

Nelson, Dawn D. (1987). "Record Linkage v. Confidentiality from the Perspective of the U.S. Bureau of Census," Protection of 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.

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

Onsrud, H.J. (1992a). "In Support of Open Access for Publicly Held Geographic Information." GIS Law. 1.1: 3-6.

Onsrud, H.J. (1992b). "In Support of Cost Recovery for Publicly Held Geographic Information." GIS Law. 1.2: 1-7.

Onsrud, Harlan (1993). "GIS and Privacy". GIS/LIS '93. Minneapolis, MN

Pearson, Hilary E. (1991). "Data Protection in Europe." The Computer Lawyer 8.8: 24.

Parker, D.B., S. Swope, and B.N. Baker (1990). Ethical Conflicts in Information and Computer Science, Technology, and Business. Wellesley, MA: QED information Sciences, Inc.

Paul v. Davis (1976) 424 U.S. 693.

Post, G. and J.D. McLaughlin (1993). "Developing the Spatial Information Marketplace: A Canadian Case Study" 277-292 in Masser, I. and H. Onsrud, eds., Diffusion and Use of Geographic Information Technologies. Dordrecht, Netherlands: Kluwer Academic Publishers.

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

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

Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974), Pub. L. No. 94-394, 90 Stat. 1198 (1976), Pub. L. No. 95-38, 91 Stat. 179 (1977), Pub. L. No. 100-503, 102 Stat. 2513 (1988)

Privacy and 1984: Public Opinions on Privacy issues, Hearings Before a Subcommittee of the House Committee on Government Operations, 98th Congress, 1st sess. 16 (1984)

Privacy Protection Act of 1980, Pub. L. No. 96-440, 94 Stat. 1879-1883 (1980)

Privacy Protection for Rape Victims Act of 1978, Pub. L. No. 95-540, 92 Stat. 2046 (1978)

Prosser, William L. (1960). "Privacy" California Law Review 48.3: 383-423.

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

Reitman, Valerie (1991). "Firms scrap plans to sell database with personal details on consumers ." The Philadelphia Inquirer Jan. 24, 1991: 1.

Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3697 (1978), Pub. L. No. 96-3, 93 Stat. 5 (1978), Pub. L. No. 96-443, 94 Stat. 1855 (1980), Pub. L. No. 97-320, 96 Stat. 1527 (1982), Pub. L. No. 98-21, 97 Stat. 83 (1983), Pub. L. No. 99-569, 100 Stat. 397 (1986), Pub. L. No. 99-570, 100 Stat. 3207-22 (1986), Pub. L. No. 100-690, 102 Stat. 4357 (1988), Pub. L. No. 101-73, 103 Stat. 438, 496, 497, 498 (1989), Pub. L. No. 101-647, 104 Stat. 4791 (1990), Pub. L. No. 102-242, 105 Stat. 2375 (1991), Pub. L. No. 102-550, 106 Stat. 4059 (1992), Pub. L. No. 102-568, 106 Stat. 4342 (1992)

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

Rotenburg, Marc (1991). "In Support of a Data Protection Board in the United States." Government Information Quarterly 8.1: 79.

Rotenberg, Marc (1993). "Communications Privacy: Implications for Network Design." Communications of the ACM 36.8: 61.

Rothfeder, Jeffrey (1992). Privacy for Sale: How Computerization Has Made Everyone's Private

Life an Open Secret. New York: Simon and Schuster. 218.

Rubin, Michael Rogers (1988). Private rights, public wrongs: the computer and personal privacy. Norwood, NJ: Ablex Publishing Corporation.

Schwartz, John (1991). "How did they get my name?" Newsweek June 3: 40- 42.

Shorter v. Retail Credit Co., D.C.S.C., 251 F. Supp. 329, 330.

Simitis, Spiros, 1987, "Reviewing Privacy in an Information Society", University of Pennsylvania Law Review. 135.3: 707-746.

Smith, Henry Jefferson (1990). "Managing information: A study of personal information privacy." Doctoral Dissertation(D.B.A.), Harvard University Business School.

Smith, Robert Ellis (1992). "About Privacy." Compilation of State and Federal Privacy Laws Providence: Privacy Journal, 5-6.

Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394 (1991) Pub. L. No. 102-556, 106 Stat. 4186 (1991)

Trubow, G. (1989). Watching the Watchers: The Coordination of Federal Privacy Policy. Washington, D.C.: The Benton Foundation.

Trubow, G.B. (1990). "Protecting Informational Privacy in the Information Society." Northern Illinois University Law Review. 10: 521-542.

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.

Tuerkheimer, Frank M. (1993). " The Underpinnings of Privacy Protection". Communications of the ACM, August. 36.8: 69-73.

Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (1988)

Wacks, Raymond (1989). Personal Information. Oxford: Clarendon Press

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