Confidentiality Issues and Policies Related to the Utilization and Dissemination of Geospatial Data for Public Health Applications

A Report to:

The Public Health ApplicationS of Earth Science Program
National Aeronautics and Space Administration
Science Mission Directorate, Applied Sciences Program

300 E Street, S.W.
Washington DC 20546

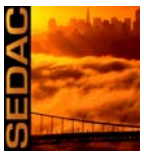
Submitted by:

The Socioeconomic Data and Applications Center (SEDAC)
Center for International Earth Science Information Network (CIESIN)
Columbia University
PO Box 1000, 61 Route 9W, Palisades, New York 10964 USA
Phone: +1 845 365-8988 Fax: +1 845 365-8922

Prepared by:

Meredith L. Golden, Robert R. Downs, and Kent Davis-Packard

March 2005



World Data Center for Human Interactions in the Environment

Columbia University in the City of New York

Confidentiality Issues and Policies Related to the Utilization and Dissemination of Geospatial Data for Public Health Applications

Table of Contents

Preface iii

Executive Summary v

Introduction 1

Privacy and Confidentiality 3

Definitions 3

Ethical Considerations 4

Legal Foundations 5

The Benefits and Risks of Disseminating Geospatial Data 10

Strategies for Protecting Confidentiality of Geospatial Data 12

Government Practices, Protocols, and Policies 16

NASA's Responsibilities, Current Activities, and Future Role 21

References 27

Appendix I: NASA Public Health Applications Program Confidentiality and Geospatial Data Workshop 37

Appendix II: American Statistical Association's Privacy, Confidentiality, and Data Security Website 40

Appendix III: Related Activities 46

Appendix IV: Selected Bibliography 56

Preface

The Socioeconomic Data and Application Center (SEDAC) has compiled for the NASA Public Health ApplicationS of Earth Science (PHASES) Program the following report on "Confidentiality Issues and Policies Related to the Utilization and Dissemination of Geospatial Data for Public Health Applications." The purpose of the report is to assist in providing the knowledge and tools necessary to manage and sustain partnerships between NASA and the public health community. The report specifically seeks "to increase the understanding of NASA administrative, legal, scientific, and technical personnel regarding confidentiality and related ethical issues in the use of geospatial data for public health purposes" (Goal #4, Public Health Applications Program for 2003-2007). The findings presented here are a result of an extensive review of the literature, interviews with researchers and governmental staff, and the presentations at the "Confidentiality and Geospatial Data Workshop" on 16 July 2003 at the National Academy of Sciences, Washington DC (NASA PHAP, 2003; see Appendix I).

The report is intended to provide a broad range of materials related to confidentiality, especially in terms of geospatial data. It includes both current and historical references to the ethical, legal, economic, and technical issues associated with confidentiality concerns. Recent journal articles, books, conference proceedings, and web sites are the basis for information on the standard procedures and policies employed by NASA and other agencies and organizations. Interviews with key government personnel regarding current confidentiality practices clarify and augment the written texts. In addition, the presentations and discussions by experts at the Confidentiality and Geospatial Data Workshop not only describe the tension between confidentiality concerns and data-sharing needs, but also suggest alternative approaches and solutions for researchers and administrators to consider.

This report was prepared by SEDAC staff members Meredith L. Golden, Robert R. Downs, and Kent Davis-Packard, with inputs from SEDAC Manager Robert S. Chen and lead SEDAC Project Scientist Deborah Balk. We thank the former PHASES Program Manager, Dr. Robert A. Venezia, for his encouragement and support, and Dr. John Haynes, the current Program Manager, for his continued interest. We also thank the participants in the Confidentiality and Geospatial Data Workshop for their interest and inputs and the U.S. National Committee for CODATA for hosting the workshop at the National Academy of Sciences.

This work was supported by NASA under contract NAS5-03117. The opinions expressed in this report are those of the author and are not necessarily the viewpoints of CIESIN, Columbia University, or NASA.

Executive Summary

The synthesis of geospatial data with socioeconomic and medical data promises to provide many benefits for society, especially in terms of improving public health. Geographic Information Systems (GIS) are powerful integrating technologies capable of bringing together information from a variety of sources, including remotely sensed data from instruments aboard aircraft and orbiting satellites and precise spatial coordinates from Global Positioning System (GPS) instruments. As demonstrated in the National Research Council publication, *People and Pixels: Linking Remote Sensing and Social Science* (NRC, 1998), the analytical potential of linking spatially explicit data with health surveys and other demographic and behavioral data is great. However, location-specific data at the household or even neighborhood level may provide sufficient information so that the identity of study subjects can either directly or indirectly be determined. Thus, individuals on whom data have been collected may rightfully fear that the integration and dissemination of data with georeferenced identifiers will compromise confidentiality and violate their privacy (Doyle *et al*., 2002).

In the field of public health, good science and successful policies depend on developing effective strategies to balance the rights of individuals with the needs of the community. In order to understand, diagnose, monitor, treat, and prevent diseases and injuries that harm sectors of the population, it is necessary to enlist the cooperation of those at risk. Only with detailed information on individual exposures, behavior, and socio-demographic and health conditions can researchers begin to understand the etiology of illnesses. Survey and study data combined with extensive georeferenced data from multiple projects across diverse disciplines can further reveal the dynamic interactions of environment, infrastructure, populations, and disease. However, such linkages also have the potential of disclosing the identities of individual study participants.

Given the sensitivity of health and socioeconomic information, the public are justly concerned about possible disclosures. Leakages about health status could jeopardize an individual's employment, insurance benefits, and social acceptance (Hyman, 2000). Consequently, threats of lawsuits and political backlash have thwarted academic institutions and government agencies from sharing valuable datasets and maximizing their utility for the benefit of public health. Although recent technological advances in information science can greatly assist in the battle against disease, no progress will be made unless effective strategies are developed and implemented to protect data confidentiality.

Many government agencies, institutions, and other organizations that use geospatial data have begun to address confidentiality concerns and to develop plans and policies to ensure its protection. The first step is to make sure that researchers and administrators understand the rewards and risks of using geospatial data in combination with personal information. The rewards include scientific progress in the area of public health. The risks are the potential harm to individual study participants or communities by disclosing sensitive information, which may also make the researchers or data providers liable for monetary or other losses. Once scientists and other staff understand how these costs and benefits relate to their own

work, then they can help develop and implement appropriate measures to minimize the disclosure of confidential data and maximize the utilization of geospatial data.

In recognition of the importance of confidentiality issues, the NASA Public Health Applications Division sponsored the Confidentiality and Geospatial Data Workshop, organized by SEDAC on July 16, 2003 at the National Academy of Sciences in Washington DC. NASA (see Appendix I) scientists and administrators involved with geospatial data projects and experts from other agencies, academia, and the private sector participated in the workshop. Presentations encompassed the ethical, legal, agency, research, and commercial aspects of confidentiality issues, and the panel discussions addressed key conflicts between geospatial data-sharing and privacy issues. The workshop participants agreed on the need to tackle these problems and considered existing tools, policies, and procedures for restricting access to and limiting disclosure of confidential data.

Some approaches that have been implemented to protect confidentiality while still providing data access include: aggregation, masking, and suppression; research contracts with confidentiality clauses and disclosure penalties; “safe houses” for restricted data access by approved users; and, protected online data-sharing collaboratories. Although NASA has established confidentiality policies for human subjects partaking in space-related research, it will be necessary to further refine and tailor these and other strategies in order to preserve confidentiality and fulfill research objectives related to initiatives that specifically combine geospatial data with individual socioeconomic and health characteristics. Once confidentiality issues and solutions are better understood, it will be possible for NASA staff to collaborate with other agencies and institutes to jointly develop and implement appropriate and effective policies for the utilization and dissemination of geospatial data for public health applications.

Introduction

The utilization of geospatial data coupled with computer technology enables researchers and decision makers to better understand the dynamic relationships among critical factors in research across many disciplines, including the health sciences. Developments in remote sensing and computing technology have improved the resolution of geospatial data and facilitated the integration of these data with other data, offering greater analytical capabilities for research and practice. Phillips *et al.* (2000) state that, though underutilized, "Geographic information systems are powerful tools for combining disparate data in a visual format to illustrate complex relationships that affect health care access. These systems can help evaluate interventions, inform health services research, and guide health care policy."

Geospatial data analysis has contributed to studies in health care delivery, epidemiology, disease ecology, and environmental health (Kistemann *et al.,* 2002). Combining geospatial data with health data has resulted in the development of systems that improve access to health information (Buckeridge *et al.,* 2002). Although higher resolution data and enhanced computing capabilities contribute to the potential utility of combining geospatial data with health data, the confidentiality of information that identifies individuals and households is more difficult to protect (Cox, 1996). Thus, the risk of compromising the confidentiality of health data used in concert with geospatial data could offset the potential benefits of using geospatial data for health science research (O'Dwyer and Burton, 1998).

Federal laws and regulations that mandate protections for the privacy of citizens are applicable to the use of geospatial data. The Office of Management and Budget (OMB) states in "Circular A-16 Revised: Coordination of Geographic Information and Related Spatial Data Activities" that geographic and spatial data must not compromise the privacy and the security of personal data about citizens (US OMB, 2002). The Health Insurance Portability Accountability Act (HIPAA, 1996) also has increased the restrictions for sharing and disseminating patients' health information to protect their privacy (US DHHS/NIH, 2003b). However, many government agencies are required by the Freedom of Information Act (FOIA, 1996) to make information, critical to the welfare of individuals and collected/recorded with taxpayers' dollars, available to the public, including researchers and decision makers (US DOJ, 2002). Thus, a tension exists between an individual's "right to privacy" and an individual's "right to know." It is the responsibility of the government to balance these competing values in such a manner that is acceptable to our society: preserving confidentiality, but still contributing to the public good.

Recognizing the need to increase awareness of confidentiality and related issues when using spatial data, the NASA Public Health Applications Program (now the Public Health ApplicationS of Earth Science, or "PHASES" Program) sponsored a workshop on July 16, 2003 at the National Academy of Sciences (NASA PHAP, 2003; see Appendix I). The Confidentiality and Geospatial Data Workshop was organized by SEDAC to bring together leading experts from government agencies, research universities, and commercial organizations to discuss issues of confidentiality pertaining to the use of spatial data.

Morning speakers at the workshop presented agency, researcher, legal, ethical, and commercial perspectives on the use of spatial data that either contain or could be matched with confidential information. The afternoon sessions consisted of two panels. The Government Agency Panel focused on confidentiality concerns related to the use of spatial data and how such concerns have been addressed by different agencies. The members of the Researchers Panel described: 1) the benefits of integrating geospatial data with other data; 2) potential compromises to confidentiality from such practices; and 3) approaches and plans for preventing breaches to confidentiality. Workshop participants suggested that steps should be taken to make key personnel within government and research centers fully aware of confidentiality issues. In addition, they concluded that effective practices and procedures must be identified and implemented to secure the confidentiality of data while maximizing its utilization.

Privacy and Confidentiality

Definitions

Although often applied interchangeably, the terms "privacy" and "confidentiality" have distinct definitions (Mayer, 2002: 3) that become crucial when the issue of maintaining individuals' ethical and legal rights is concerned. According to the President's Commission on Federal Statistics, "privacy" is defined as "the individual's right to decide whether and to what extent he will divulge to the government his thoughts, opinions, feelings, and facts of his personal life" (President's Commission, 1971: 197). However, "confidentiality" refers to "the transmittal of personal information by someone other than the identified individual." The Commission states that confidentiality restrictions "should always mean that a) Disclosure of data in a manner that would allow public identification of the respondent or would in any way be harmful to him is prohibited; and b) Data are immune from legal process" (President's Commission, 1971: 222).

Some of the earliest references to privacy and confidentiality concern the safeguarding of health information. The Hippocratic Oath from the 5th century B.C. addresses the responsibility of the physician to maintain the confidentiality of patient information (Madsen, 2003). In the *Journal of Law, Medicine & Ethics*, Rothstein (1998: 198) defines privacy as:

> *…the limited access to a person, the right of an individual to be left alone, and the right to keep certain information from disclosure to other individuals. Privacy would encompass an individual's right to decide whether to receive certain information about himself/herself from a third party. It would also involve the circumstances under which the individual shares information with others, such as family members, health care providers, or entities with a financial interest in the individual's current or future health, including an employer or an insurer.*

By contrast, Rothstein defines confidentiality as "the right of an individual to prevent the redisclosure of certain sensitive information that was disclosed originally in the confines of a confidential relationship. The paradigmatic confidential relationship involves the patient and physician" (Rothstein, 1998: 198).

"Informational privacy" is a relatively new term, pertaining more and more to the potential for vast amounts of personal information to be rapidly disseminated by electronic means. Duncan, Jabine, and de Wolf (1993) explain that informational privacy refers to "an individual's freedom from excessive intrusion in the quest for information and an individual's ability to choose the extent and circumstances under which his or her beliefs, behaviors, opinions, and attitudes will be shared with or withheld from others." Informational privacy is violated "whenever another party has access to one's personal information…Such a loss may be entirely acceptable and intended by the individual, or it may be inadvertent, unacceptable, and even unknown to the individual" (IOM, 1994: 143-144). Protection of privacy and confidentiality has taken on a new dimension and urgency in today's Information Age.

Ethical Considerations

In *Exploring the Tension between Privacy and the Social Benefits of Governmental Databases*, George T. Duncan emphasizes both ethical and pragmatic reasons why individual confidentiality should be maintained. "Ethically," he writes, "agencies ought to respect individual dignity and protect the personal information entrusted to them. Pragmatically, without attention to individual autonomy agencies will find it difficult to enlist the voluntary cooperation that smoothes operations" (Duncan, 2003: 16). Others concur on this point. Cox (1996: 1896) offers three reasons for organizations to assure the confidentiality of data from individuals:

> *First, confidentiality preservation is regarded as ethical statistical practice (International Statistical Institute, 1986: 227-242). Second, confidentiality preservation may be required by law or regulation or by organization policy [see US OMB/FCSM, 1994]). Third, it is believed that respondents would not divulge confidential information truthfully or completely without assurance of confidentiality preservation.*

Thus, guarantees of confidentiality facilitate the recruitment, honesty, and reliability of study subjects, all essential for scientific and health research. However, the ethical responsibility to maintain individuals' confidentiality is not always first in the minds of researchers, especially when data are shared across disciplines.

The capabilities resulting from geospatial data analysis raise ethical problems for collaborators sharing geospatial data (Olvingson *et al.*, 2003). The conflict is heightened with fine-grain, geographically detailed data (Rindfuss, 2002). Given that the protection of patients' health information is a primary objective for the public and for health professionals (Clough *et al.*, 1999), the benefits of employing geospatial data to health care management are being reconsidered (Foley, 2002). There is concern that privacy constraints may limit the research that can be conducted on databases containing personal identifiers and health information (Hyman, 2000). Requirements for maintaining the confidentiality of remote sensing data could result in access restrictions (Rindfuss and Stern, 1998). Thus, fears of disclosing confidential information may jeopardize scientific practices, including those of researchers and data providers.

The risks of providing access to private information must be considered in light of potential benefits. Despite threats to privacy, "labor advocates have supported occupational disease reporting as a prelude to interventions that could protect workers from hazardous work site conditions. Similarly, cancer activists have viewed tumor registries as crucial to research that could lead to intervention or treatment" (Bayer and Fairchild, 2000: 1899). However, name- and location-based reporting for surveillance and registries is often criticized by advocates for patients who are socially vulnerable such as immigrants or those with stigmatizing diseases such as HIV/AIDS. Making information with individual identifiers publicly available has the potential of compromising the privacy of listed individuals, unless appropriate measures are taken.

Both the right to privacy and the right of public access to information not only have an ethical basis, but are also rooted in our nation's origins. James Madison is attributed with the

statement: "Knowledge will forever govern ignorance, and a people who mean to be their own governors, must arm themselves with the power knowledge gives." In the book, *Private Lives and Public Policies*, Duncan *et al.* (1993) contend, "Private lives are requisite for a free society." However, the authors also state, "In a free society, public policies come through the actions of the people…Data…are the factual base needed for informed public discussion about the direction and implementation of these policies." In a recent article, Duncan (2003: 10) explains:

> *Broad access to data supports democratic decision-making. Access to government statistical information supports public policy formulation in areas ranging through demographics, crime, business regulation and development, education, national defense, energy, environment, health, natural resources, safety, and transportation.*

Despite the contradictory nature of privacy/confidentiality and open access to information, citizens expect government policies and practices to guarantee both rights.

Legal Foundations

As part of the NASA Confidentiality and Geospatial Data Workshop (NASA, PHAP, 2003), Dr. Joanne Gabrynowicz, director of the National Remote Sensing and Space Law Center at the University of Mississippi School of Law, presented "Data, Information, Confidentiality and the Legal Landscape" (Gabrynowicz, 2003). She presented a comprehensive review of the legal foundation that provides the underpinnings of today's privacy and confidentiality laws and policies. Although there is no explicit right to privacy in the US Constitution, its constitutional foundation is based on various amendments to the Bill of Rights (IOM, 1994: 15). The 4th Amendment of the US Constitution guarantees the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." In addition, the "Penumbra" rights of the 14th Amendment safeguard the privacy of intimate activities. In 1890, Justice Louis D. Brandeis co-authored a legal opinion that cemented the right to privacy as the basis for civil action (Warren and Brandeis, 1890). Common law, including civil law torts, defends "freedom from intrusion into fundamental, personal, intimate aspects of lives." Under the "tort of privacy," personal privacy is protected from offensive publicity of private facts (Gabrynowicz, 2003). The Constitution itself only provides weak and limited protection of the confidentiality of individual health care information; most of the relevant rulings are based on the interpretation of the Constitution through case law. Several key laws, enacted over the past three decades, provide general privacy and confidentiality requirements that either directly or indirectly affect all government agencies. These include The Privacy Act of 1974, The Computer Security Act of 1987, Health Insurance Portability and Accountability Act of 1996 (HIPAA), US Patriot Act of 2001, and The Confidential Information Protection and Statistical Efficiency Act of 2002.

Privacy Act of 1974 and Computer Security Act of 1987

Individually identifiable or confidential data collected or used by Federal agencies are protected under two key laws: the Privacy Act (1974) and the Computer Security Act (1987; Seastrom, 2002). The Privacy Act of 1974, overseen by the Office of Management and Budget (OMB), provides lawful regulations on issues concerning the individual's interest in personal information and the information collected by the Federal Government. Basically,

the Act ensures individuals "the right to know about, challenge, control, and correct information about oneself in federal government databases" (IOM, 1994: 15). It also "prohibits the use of information for a purpose other than that for which it was collected without the consent of the individual" (US Congress, OTA, 1986: 4). Federal agencies must adhere to specific requirements that protect both the confidentiality and integrity of personal data and restrict the use of such data. Instructions on how to guard individually identifiable data according to Federal statutes and regulations were presented in May 1975 as part of "The Federal Information Processing Standard Publication 41, Computer Security Guidelines for Implementing the Privacy Act of 1974" (US DOC/NBS, 1975), but later withdrawn in November 1998.

The implementation of the Privacy Act has been plagued by several problems (US Congress, OTA, 1986). First, only a few agencies have revised their privacy guidelines to take into account advances in information accessibility due to microcomputers. Second, there has been little analysis of the cost and effectiveness of measures designed to prevent the matching of online databases and subsequent disclosure of individual identifiers. Finally, most Federal Agencies assign less than one person-year to issues of privacy.

In 1987 Congress passed the Computer Security Act to further protect "sensitive information" including "any unclassified information that could adversely affect the national interest, the conduct of Federal programs, or individual privacy covered by the Privacy Act of 1974" (Seastrom, 2002). Under this law, Federal agencies must develop and execute security plans to safeguard computers hosting sensitive information.

HIPAA Privacy Rule, 1996

The Department of Health and Human Services (DHHS) issued the Standards for Privacy of Individually Identifiable Health Information, "The Privacy Rule" (US DHHS/OCR, 2002; US DHHS/NIH, 2003b), in response to requirements under the Health Insurance Portability and Accountability Act of 1996 (HIPAA, 1996). The Privacy Rule became effective on April 14, 2003. It provides the first comprehensive Federal protection for the privacy of personal health information. The Standards govern how certain health care providers, health care clearinghouses, and health plans use and disclose identifiable health information. The DHHS Office for Civil Rights hosts the HIPAA Privacy Website, http://www.hhs.gov/ocr/hipaa (US DHHS/OCR, 2003). The site provides background information, educational materials, and HIPPA regulations and standards, including the full text of the Privacy Rule mandated by HIPAA. The OCR is the entity responsible for the implementation and enforcement of the privacy regulations.

USA Patriot Act, 2001

Since the terrorist assaults of September 11, 2001, legislation has both increased government access to information that had been considered confidential and decreased citizen's access to information that had been considered public. The Patriot Act, formally known as "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" (USA Patriot Act, 2001), was signed by President George W. Bush on October 26, 2001. Sections 210 and 211 enable government officials to subpoena Internet Service Providers, without a court review, and force them to hand over "records of internet

times and durations, temporarily assigned network (I.P.) addresses, and means and source of payments—including credit card or bank account numbers" (Duncan, 2003: 9). At the same time, the National Defense Authorization Act and the Public Health Security and Bioterrorism Preparedness and Response Act restrict the materials that agencies are permitted to release under the Freedom of Information Act. Access to some information that had been available online, such as detailed maps of watersheds and nuclear power plants, is now restricted.

Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA)

The primary purpose of the E-Government Act (2002) is:

> *…to enhance the management and promotion of electronic Government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services, and for other purposes.*

It is noteworthy that Congress saw it necessary to include as Title V of this Act, the Confidentiality Information Protection and Statistical Efficiency Act of 2002 (CIPSEA, 2002). Subtitle A—Confidential Information Protection ensures that:

1) *information supplied by individuals or organizations to an agency for statistical purposes under a pledge of confidentiality is used exclusively for statistical purposes;*
2) *individuals or organizations who supply information under a pledge of confidentiality to agencies for statistical purposes will neither have that information disclosed in identifiable form to anyone not authorized by this title nor have that information used for any purpose other than a statistical purpose; and*
3) *the confidentiality of individually identifiable information acquired under a pledge of confidentiality for statistical purposes by controlling access to, and uses made of, such information.*

The rule for use of data or information for nonstatistical purposes is that the statistical agency or unit must "provide notice to the public, before the data or information is collected, that the data or information could be used for nonstatistical purposes." Those agencies designated statistical agencies affected by the Act are the Bureau of the Census (Commerce), Bureau of Economic Analysis (Commerce), and the Bureau of Labor Statistics (Labor). In implementing the Act (CIPSEA, 2002), these Bureaus must ensure confidentiality by:

1) *emphasizing to their officers, employees, and agents the importance of protecting the confidentiality of information in cases where the identity of individual respondents can reasonably be inferred by either direct or indirect means;*
2) *training their officers, employees, and agents in their legal obligations to protect the confidentiality of individually identifiable information and in the procedures that must be followed to provide access to such information;*

3) *implementing appropriate measures to assure the physical and electronic security of confidential data;*

4) *establishing a system of records that identifies individuals accessing confidential data and the project for which the data were required; and*

5) *being prepared to document their compliance with safeguard principles to other agencies authorized by law to monitor such compliance.*

Although only the designated agencies are required to adhere to these "safeguard principles," how they deal with the requirements set for individually identifiable data might help other agencies develop their own policies and protocols.

Coordination of Geographic Information and Related Spatial Data Activities, OMB Circular No. A-16, 2002 Revision

In 1990, the Office of Management and Budget revised Circular No. A-16 (US OMB, 1990) to address how Federal agencies should coordinate Federal surveying, mapping, and related spatial data and to begin the development of a national digital spatial information resource. It established the Federal Geographic Data Committee (FGDC), an interagency coordinating committee chaired by the Department of the Interior to coordinate related activities. The 2002 Revision of Circular No. A-16 describes in detail the National Spatial Data Infrastructure (NSDI) and provides additional "direction for federal agencies that produce, maintain or use spatial data either directly or indirectly in the fulfillment of their mission" (US OMB, 2002). It mandates that respect for privacy must be honored as a "key public value" in establishing the National Spatial Data Infrastructure (NSDI). All agencies that collect, use, or generate geospatial data must protect the "privacy and security of citizens' personal data and accuracy of statistical information on people, both in raw form and in derived information products." However, the revised circular also guarantees another "key public value" – "access for all citizens to spatial data, information, and interpretive products, in accordance with OMB Circular A-130, [US OMB, 2000a]." How OMB addresses and resolves potential conflicts between these two public values could provide a valuable blueprint for other agencies.

Most existing laws fall short of fully protecting privacy and confidentiality of electronic data. The primary issues concern the comprehensiveness and consistency of coverage (IOM, 1994: 17). Variations in the extent to which confidentiality must be preserved depend upon the type and holder of the information. Laws related to health care records vary greatly within and across state lines. In the past, few regulations have prohibited the redisclosure of confidential health data to additional parties. Once consent was given for the initial release, patients no longer could control to whom or for what purpose their information is distributed. Although the Health Insurance Portability and Accountability Act (HIPPA, 1996) supposedly gives patients more control over their health information, many patients feel they must relinquish their rights in order to receive treatment or insurance benefits. Even when a patient refuses to permit the dissemination of his or her health information, it may be too difficult or costly to enforce. Duncan (2003: 8) suggests that there is hope that new laws, such as Title V of the E-Government Act of 2002, The Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA, 2002), as described above, will help secure highly sensitive, distributed government databases whose records can be potentially linked.

To be effective, new laws must take into account the heterogeneity of the types of data covered, the complexity and variations in the information systems, the differences in management at the multiple sites, and the goals and regulations of the specific data agencies.

The Benefits and Risks of Disseminating Geospatial Data

The Information Age has revolutionized the capacity of scientists, policymakers, and the public to understand and to address many key issues. The increased utilization of new digital instruments, such as Geographic Information Systems (GIS) and remote sensing, has greatly improved the processing, analysis, and visualization of spatial data (Kistemann *et al*., 2002). Huge amounts of data can be collected, stored, transferred, integrated, analyzed, disseminated, and retrieved quickly and relatively inexpensively through distributed computer systems worldwide (Doyle *et al*., 2002: ix). Efficient systems have also been developed to match large databases based on information regularly available in individual records and to extract information based on the user needs. The research and application potential is unprecedented.

Progress in achieving health for all depends upon effectively collecting, integrating, and utilizing medical, public health, socioeconomic, environmental, and physical science data. With the advent of Internet access and the collection of geospatial data, there exists the potential to address a wide spectrum of health issues plaguing today's populations. Charles M. Croner, of the Office of Research and Methodologies at the Centers for Disease Control and Prevention's (CDC) National Center for Health Statistics, foresees the future of public health research and actions closely connected to advances in information technology (Croner, 2003):

> *Increasing Web resources from distributed spatial data portals and global geospatial libraries, and a growing suite of Web integration tools, will provide new opportunities to advance disease surveillance, control and prevention, and insure public access and community empowerment in public health decision-making. Emerging supercomputing, data mining, compression and transmission technologies will play increasingly critical roles in national emergency, catastrophic planning and response, and risk management.*

These information tools and resources enhance the ability of researchers to explore data, identify patterns, and test hypotheses. The resulting advances will enable policymakers to more effectively monitor changes in community health, develop prevention strategies, and target population subsets for effective intervention and treatment.

Although new technological advances can empower individuals and neighborhoods seeking resources for better health care, they have also heightened concerns about individual privacy and confidentiality. These rights could easily be violated given the new capabilities in amassing large amounts of detailed personal information from multiple sources and distributing it rapidly to unlimited recipients. Innovations in data access, linkages, and searches have increased the risk of disclosure; however, few agree on the extent and gravity of such risk (NSF Workshop, 2003). Concerns for data confidentiality have led to questions about the security of the methods used to create hybrid data applications and products by combining geospatial data with other forms of data, such as population and socioeconomic data (Martin and Higgs, 1997). Without sufficient understanding of the risk of disclosure, many oversight committees consistently limit data sharing, even for research purposes.

On behalf of the Panel on Institutional Review Boards, Surveys, and Social Science Research, the Chair, Coral Marrett, wrote in a letter to the Committee on Assessing the System for Protecting Human Research Participants (Marrett, 2002: 2):

> *Protecting against a breach of confidentiality is imperative when it could cause substantial harm to a research participant—for example, denial of health insurance or employment because of information supplied about a medical condition. Even if no or only minimal harm is likely, a confidentiality breach could undermine the credibility of researchers and needlessly reduce the willingness of people to participate in research.*

Some study subjects may be hesitant to respond for fear that researchers might be compelled to release their personal information in a court of law (de Wolf, 2003: 70). To safeguard against otherwise compulsory legal requirements, researchers collecting or working with biomedical, behavioral, clinical, and other sensitive research can obtain "Certificates of Confidentiality" from the Department of Health and Human Services for their projects (NIH, 2002).

As discussed earlier, there are ethical and legal obligations for the government to protect the privacy of its citizens and the confidentiality of the data collected from them. In addition, public trust and the perception of confidentiality affect both data quality and response rates. The goal for government agencies is "protecting confidentiality (avoiding disclosure) but maximizing data quality and data access" (Doyle *et al*., 2002: 1). The trade-off, however, is that small reductions in the risk of disclosure may mean large reductions in the value of data for research and public policy. Good science and successful policies depend on developing effective strategies that balance the need for personal data to improve public health with the rights of privacy for individuals.

Strategies for Protecting Confidentiality of Geospatial Data

Experts agree that it is essential for data holders to develop effective strategies to protect the confidentiality of geospatial data prior to its release. The effectiveness of the strategies depends upon the type and utilization of the data and the ability of the respective authority to monitor and enforce their implementation. In recent years, much has been written on the specific challenges, designs, applications, trade-offs, and perceptions of a wide-range of strategies. Only a brief summary will be provided here with references to more detailed accounts.

There are many stages in the data process at which the government can intervene to protect the data contributor and to assist the data user (Duncan, 2003: 3):

> *Typically, government protects informational privacy by avoiding excessive intrusion as it undertakes the C stage of data capture in the CSID (Capture, Storage, Integration, and Dissemination) process. Government also explicitly promises confidentiality in the S, I, and D stages of its surveys and censuses conducted for statistical purposes.*

Strategies to protect data have been developed for each stage; however, without clear guidelines government officials may fail to implement them. Unless appropriate precautions are taken throughout the data process, agencies may feel as a last resort that the only way to ensure confidentiality is to prohibit dissemination.

In her paper, "Issues in Accessing and Sharing Confidential Survey and Social Science Data," Virginia de Wolf (2003: 66-74) reviews the practices and procedures established by the US Federal statistical system to permit others to utilize the confidential data collected by the more than 70 agencies that comprise its network. The purpose of the paper is to suggest how the social science research community could utilize these methods to safeguard confidentiality while facilitating data sharing. Much of her analysis is based on the work of three groups that have assessed the responsibilities of the Federal government as 'data steward': 1) Panel on Confidentiality and Data Access (Duncan *et al*., 1993; Jabine, 1993a, 1993b); 2) Subcommittee on Disclosure Limitation Methodology of the Federal Committee on Statistical Methodology (US OMB/FCSM, 1994); and 3) the Federal Committee on Statistical Methodology's (FCSM) Confidentiality and Data Access Committee (US OMB/FCSM CDAC, 2004). Following their terminology, de Wolf describes alternative approaches in terms of "restricted data" and "restricted access." The first refers to restricting "the content of the data prior to releasing it to the general public" and the latter to limiting "the conditions under which the data can be accessed, i.e., who can have access, at what locations, for what purposes" (de Wolf, 2003: 66).

The book *Confidentiality, Disclosure, and Data Access* (Doyle *et al.*, 2002) contributes substantially to understanding both the overall confidentiality and data access issues confronting statistical agencies and the range of alternative strategies for specific applications. It also provides an introductory background on relevant concepts and technical definitions for which it credits the Confidentiality and Data Access Committee of the FCSM. In terms of strategies to protect confidentiality, the editors describe how statistical agencies

have historically guarded confidentiality by means of data protection, statistical analysis, and various access modalities. To provide data protection, agencies alter the data by removing information that could either directly or indirectly reveal an individual's identity. Another approach is for the agency to conduct its own statistical analysis on the data and only release information on the trends observed for groups of the respondents rather than for individuals. Finally, new access modalities, including licensing agreements, remote access arrangements, and secure remote sites, offer a range of access to users while protecting sensitive data.

Prior to the public dissemination of microdata, agencies need to examine the data and make modifications when necessary to prevent the identification of individual respondents. Data protection methods range from simple cell suppression to elaborate statistical applications for entire databases. The approaches used to limit disclosure are tailored according to the type of data and the product to be disseminated. The methods differ based on whether the underlying data are microdata (individual units) or aggregate estimates (formatted as frequency counts or aggregate magnitude data) (Doyle *et al.*, 2002: 5). Different techniques are also employed depending upon the type of data product to be released—microdata files or tables (de Wolf, 2003: 67). The three most common practices that limit disclosure in microdata include 1) eliminating information that directly identifies individuals, 2) suppressing data that may indirectly identify individuals, and 3) introducing uncertainty into the reported data. Uniquely identifying characteristics can be concealed by "rounding, top- and bottom-coding, collapsing categories, and removing information such as detailed geography" (Doyle *et al*., 2002: 5).

Primary and complementary cell suppressions are utilized to prevent disclosure of confidential information from frequency count and aggregate magnitude data. Special precautions must be taken for tabular data obtained via online systems that permit users to request "tables on demand." Although disclosure may be protected for each of the individual requests, the combination of the results by outsiders could reveal individual identifiers. According to a survey of North American and European countries (Felso *et al*., 2002), most agencies use cell suppression at a threshold of 3 to protect data in frequency count tables. In the case of aggregate magnitude data, the technique referred to as the "N-K" rule is employed to determine sensitive cells that are then either eliminated or the tables reconstructed. Microdata are either strictly modified or not disseminated to the public.

Data protection techniques have become more sophisticated in order to match the challenges presented by disclosure technologies. As mentioned previously, *Confidentiality, Disclosure, and Data Access* (Doyle *et al.*, 2002) provides detailed discussions by experts for many key topics. Chapters on data protection include: "Disclosure Control Methods and Information Loss for Microdata" (Domingo-Ferrer and Torra, 2002: 91-110); "A Quantitative Comparison of Disclosure Control Methods for Microdata" (Domingo-Ferrer and Torra, 2002: 111-134); "Disclosure Limitation Methods and Information Loss for Tabular Data" (Duncan *et al*., 2002: 135-166); "Nonperturbative Disclosure Control Methods for Tabular Data" (Giessing, 2002: 185-214); and "Disclosure Limitation in Longitudinal Linked Data" (Aboud and Woodcock, 2002: 215-278).

The increasing public demand for and availability of detailed data associated with small area geographical units challenge the traditional consideration of disclosure risk (Steel and Sperling, 2001). Many of the conventional data protection methods merge together all the records within a geographic unit to generate a population that is large enough to prevent disclosure. The Census Bureau has for years required that geographical regions have at least a population of 100,000 in order for information to be released without violating "personal confidentiality" (NCHS/CDC, 2003: 3). However, the Health Insurance Portability and Accountability Act of 1996 (HIPAA, 1996) only prohibits the release of data for areas with fewer than 20,000 people, despite assertions of maintaining patient privacy. Research has shown that the percentage of the population that can be uniquely identified rises substantially with a reduction in population size (Hawala, 2000). According to Hawala, the use of a 100,000-population threshold for the release of data is necessary to protect the identity of subjects within most demographic microdata files. In order to simplify the problem and remove the need to apply other disclosure prevention methods, Steel and Sperling (2001) propose that data providers adopt a "universally agreed upon set of basic units, which are designed to be of a size appropriate for 'safely' displaying data." While the merger of geographic areas into standardized, basic units would help protect the confidentiality of individuals, it may also significantly diminish the quality and breadth of the data available to researchers and policymakers, thus compromising its potential usefulness.

The adoption of standardized geographic units and the application of other disclosure limitation methods for microdata files need to consider the degree of the disclosure risk, the potential benefits from utilization of the data, and the integrity and competency of the users. Armstrong, Rushton, and Zimmerman (Armstrong *et al.*, 1999: 497-525) suggest a variety of alternative geographical masking techniques for individual-level data. These include individual and concatenated affine transformations, random perturbation, aggregation, neighbor information, and contextual information. They propose "purpose-specific masks" rather than all-encompassing solutions: "The best approach depends on the purpose of the data user as well as the degree of risk of disclosure that the data custodian wishes to tolerate." (Armstrong, *et al.*, 1999: 500). The authors also address the relative validity and security of the data resulting from each approach. Although these methods greatly improve the utility of the data while preserving confidentiality, questions remain regarding the degree to which these masks alter the accuracy of statistical analyses.

Researchers have recommended involving the public as well as advisory boards to evaluate data release on a case-by-case basis. Olvingson *et al.* (2003: 183) advocate the creation of a forum for open discussion of these issues "to inform and educate both users and the general public." Participants at the NASA Confidentiality and Geospatial Data Workshop (NASA PHAP, 2003) also stressed the need to educate decision makers so that adequate resources can be allocated to ensure that privacy and confidentiality provisions are in place, implemented, and evaluated. According to Doyle *et al.* (2002: 3), government agencies must base their data dissemination decisions on how the public perceives and reacts to different data protection strategies.

In order to assist government agencies, the Confidentiality and Data Access Committee (CDAC) has developed a "Checklist on Disclosure Potential of Proposed Data Releases" (de Wolf, 2003: 67; US OMB/FCSM/CDAC, 1999). Once the checklists are completed they are

submitted for approval to the agency's Disclosure Review Board. The DRBs may be either formal or informal. Papers from the Joint Statistical Meetings on August 17, 2000 in Indianapolis describe in more detail the operation and purpose of DRB's (de Wolf, 2003: 67). Similarly, Institutional Review Boards (IRB's) have the responsibility of protecting human subjects whose data are being utilized by researchers. However, IRB's often lack the time, expertise, and funding to effectively review research proposals and protect patient confidentiality (Hyman, 2000: 1724; IOM, 2002: 5). The Panel on Institutional Review Boards, Surveys, and Social Science Research recommends that the Institute of Medicine Office for Human Research Protections (OHRP) "provide guidance to IRB's by documenting and promulgating good practices for maintaining confidentiality at every stage of the research process and for informing research participants about the scope and limits of confidentiality protection that is offered them" (Marrett, 2002: 2-3).

Given that data protection methods may restrict the scope of data applications, agencies have also explored practices and procedures that will prevent public disclosure, but permit more in-depth utilization of the data for academic and policy purposes. Through licensing agreements, data holders provide data for a limited time to researchers who formally agree to abide by the agency's policies and restrictions to protect the data confidentiality or be subject to penalties under law. With remote access, researchers request that the data agency run specific computer programs on the data. Prior to returning the results to the researcher, the data agency reviews them to make sure that the data confidentiality is maintained. Several chapters in *Confidentiality, Disclosure, and Data Access* (Doyle *et al.*, 2002) investigate the potential of alternative "access modalities": "Licensing" (Seastrom, 2002: 279-296), "Issues in the Establishment and Management of Secure Research Sites" (Dunne, 2002: 297-314), and "The Potential and Perils of Remote Access" (Blakemore, 2002: 315-340).

Finally, secure remote sites, such as the Research Data Centers (RDCs) set up by the US Census Bureau, the National Science Foundation, the National Center for Health Statistics, and the Agency for Healthcare Research and Quality, permit users access to data with fewer modifications (de Wolf, 2003: 69). However, the researchers must remain in controlled environments, subject to the same restrictions as the agency staff. The Center for Economic Studies at the US Census Bureau (US Census/CES, 2003) supports eight, soon to be nine, RDCs. Although Carnegie Mellon University was the first university to collaborate with the Census Bureau in establishing its Census RDC (http://www.heinz.cmu.edu/census/), it recently closed the facility in August 2004. However, a new RDC has since opened at Cornell University and another is expected to open at Baruch College of the City University of New York in 2005. Such facilities are expensive to operate and must justify their existence in terms of successful utilization.

Government Practices, Protocols, and Policies

Since 1947, the Federal government has provided guidelines to protect human subjects involved in federally-funded biomedical and behavioral research. Over time, the guidelines incorporated more rigorous safeguards and eventually were codified as part of governmental policy. In 1974, the former Department of Health, Education, and Welfare established the suite of regulations protecting human subjects as recorded in the Code of Federal Regulations Title 45, Part 46. These provisions include: Subpart A—Federal Policy for the Protection of Human Subjects (Basic DHHS Policy for Protection of Human Research Subjects); Subpart B—Additional Protections for Pregnant Women, Human Fetuses and Neonates Involved in Research; Subpart C—Additional DHHS Protections Pertaining to Biomedical and Behavioral Research Involving Prisoners as Subjects; and Subpart D—Additional DHHS Protections for Children Involved as Subjects in Research. The 1991 revision of Subpart A constitutes the common Federal Policy for the Protection of Human Subjects, also known as "The Common Rule (Federal Policy)," 56 FR 28003 (Federal Policy, 1991a; Federal Policy, 2001). Seventeen Federal agencies have formally adopted the core of these regulations, including NASA, 14 CFR 1230 (Federal Policy, 1991b).

The regulations set forth in the Common Rule do not provide rigid procedures to determine the appropriateness of research involving human subjects. Instead, they offer a framework to encourage investigators and others to carefully scrutinize and implement measures safeguarding the welfare and rights of research subjects (US DHHS/NIH, 1995). Despite the general nature of the Common Rule, President Clinton, in a Memorandum on 17 February 1994 to the Vice President and the Heads of Executive Departments and Agencies, emphasized the importance of strictly enforcing these regulations:

> *…I direct each department and agency of Government to review present practices to assure compliance with the Federal Policy for the Protection of Human Subjects and to cease immediately sponsoring or conducting any experiments involving humans that do not fully comply with the Federal Policy.* (US President/Clinton, 1994)

Although each of the Federal agencies is responsible for complying with the Common Rule, the Department of Health and Human Services has a primary role in its implementation. In 2000, human research protection functions were transferred from the Office for Protection from Research Risks (OPRR) within NIH to the newly established Office for Human Research Protections (OHRP), part of the Office of Public Health and Science (OPHS) and within the Office of the Secretary of DHHS. The OHRP provides online policy guidance, information, instructions, and sample forms to assist Federal agencies in complying with the human subjects regulations (US DHHS/OHRP, 2004).

The Common Rule (Federal Policy, 1991a) defines "human subjects research" broadly as studies involving "a living individual about whom an investigator (whether professional or student) conducting research utilizes or obtains personal data through intervention or interaction with the individual or data with identifiable private information from existing sources" (45 CFR 46.102(f)(1), (2)). "Private information" refers to:

> *…information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information that has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public (for example, a medical record).*

In order for research to be subject to this regulation, the private information must be "individually identifiable," that is, "the identity of the subject is or may readily be ascertained by the investigator or associated with the information" (45 CFR 46.102(f)(2)). The Office of Human Research Protection offers the Human Subject Regulation Decision Charts (US DHHS/OHRP, 2000a) to help clarify whether or not research activities involve human subjects or whether they are exempt from the Common Rule.

To ensure compliance with the Common Rule, every institution that is supported by a Federal Department or Agency and participates in non-exempt research involving human subjects is required to submit a written Assurance of Compliance to that Department or Agency. The Assurance is a policy statement that details the procedures the institution plans to follow in order to protect human subjects. Both the recipient of the Federal funds and the collaborating performance site institutions are required to file Assurances. In the past DHHS accepted three types of assurances: Single Project Assurance (SPA), Cooperative Project Assurance (CPA), and Multiple Project Assurance (MPA). The MPAs approved by the OHRP have also been acceptable for other Federal use.

Recently, the OHRP restructured the assurance process "to significantly reduce the administrative burden on individual institutions, other Federal departments and agencies, and the OHRP." In particular, the OHRP administrators have worked with other Federal agency staff to develop a new Federalwide Assurance (FWA) to assist different types of institutions involved in federally-supported human subjects research. The FWA, Terms of Assurance, and IRB Registration are maintained online by OHRP (US DHHS/OHRP, 2003a) and can be utilized by other Federal departments and agencies to ensure their compliance with the Common Rule. The OHRP provides online application forms for Federalwide Assurances and allows for electronic submissions (US DHHS/OHRP, 2003b). If an institution does not receive funding from DHHS and has not filed a Federalwide Assurance, then it may have to file an Assurance of Compliance directly with the Federal agency funding its research, according to the specified procedures of that agency.

Prior to receiving funding, an institution must also provide to the sponsoring agency certification confirming that the research has been reviewed and approved by an Institutional Review Board (IRB) designated under an OHRP-approved Assurance (45 CFR 46.103(f)). IRB approval requires that:

> *1) the risks are minimized and reasonable in relation to anticipated benefits;*
>
> *2) there is informed consent by the subject; and*
>
> *3) the rights and welfare of the subjects are maintained.* (Federal Policy, 1991a; U.S. President/Clinton, 1994)

The OHRP online IRB Registration is required for IRB's designated on a Federalwide Assurance for Protection of Human Subjects (US DHHS/OHRP, 2003c). Other IRB's may

register voluntarily. It is possible to search the OHRP database (US DHHS/OHRP, 2002) for approved Assurances and registered IRB's by location, organization name, and designated number. The OHRP also provides several resources on its "Policy Guidance" webpage (US DHHS/OHRP, 2003d) including an "Informed Consent Checklist" (US DHHS/OHRP, 2000b). Finally, the National Institutes of Health and other Department of Health and Human Services agencies issue "Certificates of Confidentiality" (US DHHS/NIH, 2003a) for any IRB-approved research project that collects individually identifiable personal information, the release of which could significantly harm or damage the subject. "Certificates of Confidentiality" protect the confidentiality of data collected on human research participants from compulsory legal disclosure, such as court orders and subpoenas.

Other Federal agencies have adopted their own procedures and guidelines in compliance with the OHRP regarding the protection of human subjects from whom information is derived and/or utilized as part of research specifically undertaken or supported by that agency. For example, the CDC together with the Agency for Toxic Substances and Disease Registry (ATSDR) has developed a fifty-page online document, "CDC/ATSDR Procedures for Protection of Human Research Participants: 2003" (US DHHS CDC/ATSDR, 2003). The procedures for human subjects protection detailed in this report encompass Institutional Responsibilities, Institutional Review Boards, Special Populations, Protocol Handling, and Privacy and Confidentiality Protection. Within the CDC, the Office of Science Policy and Technology Transfer (OSPTT) has established a "Human Subjects Research" home page (US DHHS/CDC/OSPTT, 2004) on its website that includes checklists, forms, documents, and training updates.

OMB has issued memorandums to the heads of Executive Departments and Agencies "to remind agencies of several privacy-related legal requirements" and "clarify how agencies should conduct" such activities. The OMB guidance communications include "Guidance on Inter-Agency Sharing of Personal Data—Protecting Personal Privacy" (US OMB, 2000b) and "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002" (US OMB, 2003). In response to these requirements, the CDC and The Council of State and Territorial Epidemiologists (CSTE) Intergovernmental Data Release Guidelines Working Group (DRGWG) has issued a detailed draft report, "CDC-ATSDR-CSTE Data Release Guidelines for Re-release of State Data" (US DHHS CDC/CSTE, 2003 Draft).

Some of the proposed guidelines and recommendations regarding personal privacy address the concerns raised in the General Accounting Office publication (GAO, 2001), "Record Linkage and Privacy: Issues in Creating New Federal Research and Statistical Information." Linda Koontz, Director of Information Management Issues at GAO, has raised additional issues, specifically concerning geo-referenced data, in her testimony on "Geographic Information Systems: Challenges to Effective Data Sharing" presented to the Subcommittee on Technology, Information Policy, and Intergovernmental Relations and the Census, Committee on Government Reform (US Congress/House, 2003). Agencies have in many cases utilized statistical techniques to protect microdata with individual identifiers. Such methods are described at length in OMB's "Report on Statistical Disclosure Limitation Methodology" (US OMB FCSM, 1994) and the Census Bureau sponsored book, *Confidentiality, Disclosure and Data Access: Theory and Practical Applications for*

Statistical Agencies (Doyle *et al.*, 2002). However, little attention has been given specifically to protecting the confidentiality of geospatial data.

Due to rapidly changing technology, government agencies are faced with the responsibility of unprecedented demands for data collection, analysis, storage, dissemination, and protection. The National Science Foundation's Digital Government program announcement recognizes the change in expectations.

> *Given the inexorable progress toward faster computer microprocessors, greater network bandwidth, and expanded storage and computing power at the desktop, citizens will expect a government that responds quickly and accurately while ensuring privacy.* (NSF, 1999; Duncan, 2003: 9)

With the large increase in the number and range of potential users, agencies have been swamped by demands for access to data (Doyle *et al*., 2002: 1-3). Policymakers require agencies to rapidly provide them with volumes of specific, in-depth information. In addition, academic researchers are now requesting detailed microdata for their studies. Federal agencies are also expected to disseminate state- and local-level administrative records to the public. These demands are complicated by the vast amount of data collected by the private sector that could be matched to the government records, thus potentially disclosing a broad range of private information on individuals. Many Federal statutes, regulations, and policies require those government agencies that collect, manage, and disseminate data to also protect privacy and confidentiality. Thus, now more than ever, Federal agencies are focusing their attention on developing and implementing practices, protocols, and policies for data-sharing that maximize the public utility of the data and minimize individual disclosure, so that the agencies can successfully fulfill their goals.

Many of the approaches mentioned in the previous section of this report are being implemented by governmental agencies. Seastrom (2002) summarizes the variety of data licensing or use agreement features that different agencies employ. According to Seastrom, the National Center for Education Statistics in conjunction with the chief statistician of the OMB has devised the protocol for the licensing system. Other agencies have adopted this approach, but modified the procedures based on their specific applications and needs. The following table outlines for several agencies the operational features of the data use agreements and licenses.

The American Statistical Association Committee on Privacy and Confidentiality promotes a greater understanding of and adherence to privacy and confidentiality policies. The Committee recognizes that "…it (is) essential to keep abreast of current regulations, recommendations, and best practices in the field. Unless these concerns are adequately addressed, the quality of data available for statistical research, and decision-making may be compromised." (ASA, 2003b). To facilitate this goal, the Committee established the "American Statistical Association's Privacy, Confidentiality, and Data Security Website" (ASA, 2003a). The website provides a unique and worthwhile collection of online links to articles, reports, guidelines, laws, ethical codes, and other related resources. It describes relevant regulations and guidelines for several Federal agencies, including Commerce, Education, Energy, Health and Human Services, Justice, Labor, and Treasury. For more detailed coverage of the practices, protocols, and policies utilized by government agencies

see Appendix II, The American Statistical Association's Privacy, Confidentiality, and Data Security Website's Guidelines for Governments; and Appendix III, Related Activities: Committees, Panels, and Workgroups, Conferences and Workshops, and Reports.

Table 1. Agency-Specific Features of Data Use Agreements and Licenses (Seastrom, 2002: 290)

Organization	**IRB Approval Required**	**Institu-tional Concur-rence**	**Security Pledges All Users**	**Report Disclo-sures**	**Security Plan**	**Security Inspec-tions**	**Cell Size Restric-tions**	**Prior approval -Reports**	**Notifica-tion of Reports**
National Center for Education Statistics		X	X	X	X	X	X	X	X
National Science Foundation		X	X	X	X	X	X	X	X
Department of Justice	X	X	X						
Health Care Financing Administration					X	X		X	
Social Security Administration	X	X	X	X			X		X
Health Care Financing Administration-National Cancer Institute					X	X		X	
Bureau of Labor Statistics-National Longitudinal Survey of Youth			X	X	X	X	X		X
Bureau of Labor Statistics- Census of Fatal Occupational Injuries			X	X	X	X	X	X	
National Institute of Child Health and Human Development	X	X	X		X	X	X		X
National Heart, Lung, and Blood Institute	X								X
National Institute of Mental Health	X	X							X
National Institute on Drug Abuse	X	X							X
National Institute on Alcohol Abuse and Alcoholism		X							X

NASA's Responsibilities, Current Activities, and Future Role

Federal agencies, including NASA, must adhere to the specific requirements of the Privacy Act of 1974. The NASA Policy Directive "Privacy Act—Internal NASA Direction in Furtherance of NASA Regulation" (NASA NPD, 2003) states:

> *NASA will fully comply with the requirements of the Privacy Act of 1974, as amended, including the Computer Matching and Privacy Protection Act of 1988, and guidance from the Office of Management and Budget (OMB).*

NASA regulations implementing the Privacy Act are published in The Code of Federal Regulations, Title 14—Aeronautics and Space, Chapter V—National Aeronautics and Space Administration, Part 1212—Privacy Act—NASA Regulations (Privacy/NASA, 1999). The Act's Instructions for NASA Employees (Subpart 1212.6) pertains primarily to information about individuals that is maintained as part of a system of records at NASA. These instructions, however, might also be considered for other data generated or maintained by NASA that could directly or indirectly reveal identifiable individual information. The NASA Procedural Requirements "Security of Information Technology" (NASA NPR, 1999) goes further to specify that the Chief Information Officer (CIO) at NASA has the responsibility of managing Information Technology (IT) within the Agency. As head of the NASA Information Resource Management (IRM) program, the CIO oversees IT security and protects the confidentiality, integrity, and availability of information resources. The CIO must ensure the implementation of the Privacy Act and the Agency's compliance with the Computer Matching and Privacy Protection Act (CMPPA, 1988). The CIO in turn may designate a Privacy Officer and delegate the implementation and oversight responsibilities.

The NASA Policy Directive for the Privacy Act (NASA NPD, 2003) prohibits NASA personnel and contractor personnel from disclosing any record that is part of a system of records to any other Federal or non-Federal person or agency without proper authorization by the NASA Privacy Act Officer. Thus, prior to participating in a computer-matching program, the Center Privacy Act Manager or appropriate Systems Manager must request permission from the NASA Privacy Act Officer. All requests to NASA for computer matching must also be reviewed by the NASA Data Integrity Board. Its membership consists of the Inspector General, the Director of the Personnel Division, the Assistant Administrator for Management Systems, the Chief Health and Medical Officer (whenever medical records considered), and the NASA Privacy Officer. The Board must approve or reject requests for computer matching and notify all parties in writing of its decisions. It must write agreements between NASA and the requesting agency when appropriate. In addition, the Board acts as a clearinghouse for relevant information and report generation for the NASA Administrator, OMB, Congress, and the public as requested.

In terms of NASA's scientific and technical information (STI), specific guidelines, procedures, and standards for its creation, acquisition, management, and dissemination are outlined under NASA Procedural Requirements (NASA NPR, 1998). "STI" refers to "the collected set of facts, analyses, and conclusions resulting from scientific, technical, and related engineering research and development efforts, both basic and applied." On the one hand, the National Aeronautics and Space Act of 1958 requires the "widest practicable and

appropriate dissemination of information concerning its activities and the results thereof." On the other hand, NASA is required to protect certain information from public disclosure, including those exempt under the Freedom of Information Act (FOIA, 1996) and those subject to the Privacy Act (NASA NPD, 2003). NASA headquarters or the Chief Intellectual Property or Patent Counsel decides whether certain types of information must or must not be released.

To safeguard human subjects as codified in the Department of Health and Human Services (DHHS) regulation 45 CFR Part 46, NASA adopted in 1990 the "Common Rule," 14 CFR Aeronautics and Space, Chapter V, National Aeronautics and Space Administration. Part 1230—Protection of Human Subjects (Federal Common Rule, 1991b). According to NASA's related Policy Directive: "All human research conducted, or supported by NASA, whether on the ground, in aircraft, or in space, will follow the provisions of NASA regulations contained in 14 CFR Part 1230 and Department of Health and Human Services (HHS) regulations contained in 45 CFR Part 46" (NASA NPD, 2002). On August 8, 1995, NASA released the NASA Management Instruction (NMI 7100.8B, 1995) as its revised NASA human subjects research policy, incorporating the requirements of the Common Rule and the recommendations of the President's Advisory Committee on Human Radiation Experiments (US President ACHRE, 1995). Personnel from NASA-Johnson Space Center, NASA-Ames Research Center, and a special NASA Bioethics Policy Task Force had worked together to review existing policies and recommend additional safeguards for the NMI. At the time, the Department of Energy praised the new NASA policy as "a model for any organization conducting traditional and non-tradition biomedical research…" (US DOE, 1996). The NMI was replaced by a series of NASA Policy Directives, most recently in 2002. NPD 7100.8D (NASA NPD, 2002) updates NASA's basic policies for human subject protection and provides Agency guidance to its IRBs. Under the NPD, the Chief Health and Medical Officer (CHMO) at NASA Headquarters is ultimately responsible for the protection of human subjects; the CHMO must ensure that the Administrator, the relevant Enterprise Associate Administrator, the Office of Safety and Mission Assurance, the NASA General Counsel, and the NASA Inspector General (when appropriate) are informed via official channels of significant issues and actions.

According to the 2002 Policy Directive 7100.8D (NASA NPD, 2002), all research involving human subjects "will be reviewed by an Institutional Review Board (IRB), approved by NASA or the Office of Human Research Protection (HRP) at HHS." The Directive states that IRBs will be established at NASA Centers to review "all ground-based and aeronautical flight research, involving human subjects, that is conducted at the Centers or which utilizes NASA Centers, equipment, or personnel." Center Directors are given the responsibility of "establishing an IRB at their respective Centers." However, in contrast to the NASA NPD 7100.8D (2002), the NASA Procedural Requirements NPR 7100.1 (NASA NPR, 2003) give the Centers, except for the Johnson Space Center, the option of either setting up their own IRB *or* by prior agreement utilizing another NASA IRB to review their research proposals using human subjects.

The NASA Procedural Requirements "Protection of Human Research Subjects," NPR 7100.1, 1.5 (NASA NPR, 2003) does provide detailed procedures regarding the

establishment and operations of IRBs, such as the membership requirements, delegation of responsibilities, and preparation and maintenance of records. The NPR also requires that the Authorized NASA Official (ANO) develop and administer a NASA Human Protection Training Program in accordance with the requirements for Federal funding by the Department of Human and Health Services (DHHS). Such training is mandatory for NASA IRB members and investigators receiving funding from NASA or involved in NASA-sponsored research that involves human subjects. In addition, the IRBs are required to maintain documentation of their activities in a secure database and to make these accessible to authorized NASA representatives. In order to qualify for IRB approval, Principal Investigators must, in addition to other requirements, provide safeguards for the protection of "the privacy of subjects and the confidentiality of data, especially electronically stored data" (NASA NPR, 2003).

The 2003 NASA NPR specifically outlines the requirements for the NASA Flight IRB at the NASA Johnson Space Center. The Flight IRB must review:

> *1) all research proposals that propose the use of crew members as research subjects and/or research technicians;*
>
> *2) all space flight or aircraft research proposals that use noncrew human research subjects;*
>
> *3) all aircraft research proposals that use noncrew as research technicians if it is deemed that their participation could effect their health or safety; and*
>
> *4) all space flight or aircraft research proposals that use animals, biological, or toxic materials that could be expected to interact with the humans onboard the space or aircraft.* (NASA NPR, 2003)

The Flight IRB may also evaluate other proposals as determined by the Authorized NASA Official (ANO).

The "Johnson Space Center Institutional Review Board Guidelines for Investigators Proposing Human Research for Space Flight and Related Investigations, Space and Life Sciences Directorate (JSC-20483)" (NASA JSC, 1996) provides researchers with a "NASA/JSC Human Research Informed Consent" form (NASA JSC, 2002). It covers pre-flight, flight, and post-flight research. Study participants must provide informed consent in order to participate as test subjects in research studies, tests, investigations, or other evaluation procedures. According to its regulations, Principal Investigators are required to submit to the IRB and to the participants a detailed description of the investigation in lay terms. They must include "a statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained." Personal information from these studies "except as provided for by Agency-approved routine uses under the Privacy Act" cannot be disclosed unless "a life-threatening abnormality is detected" in which case the investigator will notify both the study participant and the JSC Flight Medicine Clinic. After receiving all the required information from the PI, the IRB then determines whether the study constitutes a "minimal" or "reasonable" risk to the employees.

The detailed attention given to the Johnson Space Center IRB may well be due to its review in 2001 by the NASA Office of Inspector General. The findings are presented in the "Assessment of the Institutional Review Board for Human Subject Protection at the Johnson Space Center, G-01-002" (NASA OIG, 2001). The basis for the review was to see whether the NASA IRBs had problems similar to the medical and research facilities funded by DHHS and Veterans Affairs. At the time, only Johnson Space Center and Ames Research Center, of all of the NASA Centers, maintained active IRBs. The Inspector General's Office chose to examine the JSC IRB because "it receives the most proposals for NASA funded biological research and reviews all experimental protocols involving humans that are to be performed on the Agency's air and space platforms." The audit found that "in general, the Johnson IRB was timely, well-organized, and staffed with qualified, hardworking individuals." However, it disclosed several concerns regarding the heavy workloads and competing priorities of IRB members and suggested improvements related to "updates in Agency policy, timely education and training opportunities for IRB members, and periodic review of the IRB process relating to research involving human subjects sponsored by Johnson." In all, the assessment presented NASA with six recommendations for improving the JSC IRB. The ultimate goal was to incorporate these suggestions into an updated Agency policy. The NASA Policy Directive, NPD 7100.8D (NASA NPD, 2002), Procedural Requirements, NPR 7100.1 (NASA NPR, 2003), and Procedures and Guidelines, NPG 7100.1 (NASA NPR, 2003) fulfill this objective.

Despite the detailed guidelines for establishing Institutional Review Boards, most of the NASA Centers do not have active IRBs. It is unclear whether there is no perceived need for IRB review at these Centers or whether arrangements have been made for reviews at the JSC or Ames IRBs. Unlike the Department of Health and Human Services (DHHS), NASA does not make available over the Internet any documents that summarize NASA IRB activities. A search of the NASA webpages yielded just two results regarding IRBs, besides the references to the actual Policy Directive and Procedural Requirements. The Ames Research Center website's "Life Scientists at Ames" (NASA Ames, 2004) mentions the IRB in reference to a study by Robert T. Whalen in which female subjects were recruited "with NASA Ames' Institutional Review Board (IRB) approval." The same webpage notes that Dr. Whalen was unable to work on another project for which he was co-PI due to "differences in IRB policy between NASA and institutional IRBs." The few references indicate both the paucity of easily accessible information on NASA IRBs and the difficulties in collaborative research that can arise without better coordination of IRBs.

In the past, NASA has demonstrated its commitment to protecting the confidentiality of medical data with extensive protocols restricting the disclosure of data generated from its research programs involving human subjects. The Inspector General's Assessment (NASA OIG, 2001) specifically defines a "research protocol" subject to review by the NASA IRBs as "a detailed plan of scientific or medical experiment, treatment, or procedure." However, it goes beyond traditional biomedical, clinical, and other scientific protocols and expands the list of human subjects research:

- *Collection and use of personally identifiable information, such as genetic information or medical and exposure records, even if the information was collected previously for a purpose other than the current research.*

- *Collection of personally identifiable data, including surveys or questionnaires, through direct intervention or interaction with individuals.*
- *The search for generalizable knowledge about categories or classes of subjects (e.g. linking job conditions of worker populations to hazardous or adverse health outcomes.*

NASA gathers and studies large collections of images, most notably via satellites. These data when matched with other datasets could reveal, either directly or indirectly, individually identifiable private information. The collection, maintenance, and analysis of these images, therefore, constitute research with human subjects under the Common Rule and are subject to its regulations whether the data are utilized directly by NASA or by others to whom NASA provides the imagery.

In order to ensure that NASA administrators and researchers comply fully with the Federal regulations regarding privacy and human subjects, it is imperative that NASA provides policy directives and procedural requirements that specifically address issues pertaining to geospatial data. Since other Federal agencies are grappling with similar concerns, it would be useful for NASA to consider the lessons they have learned from recent activities, including workshops, conferences, and committee meetings. (See Appendix III). NASA could also actively participate in the planned National Research Council study by the Committee on Human Dimensions of Global Change on confidentiality issues arising from integration of remote sensing and social science data.

NASA administrators, scientists, and staff need to work together to evaluate the current applications of and restrictions on geospatial data. To begin with, the NASA ANO should identify those internal datasets with geo-referenced attributes that could either solely or in concert with other data lead to the disclosure of individually discernible information. The extent to which and for what purposes these datasets are disseminated to other government agencies, academic researchers, and the public should also be determined. NASA must examine how its IRBs have dealt with research protocols involving geospatial data with individual identifiers in order to compare NASA's procedures with those of selected Federal agency IRBs, such as the Department of Health and Human Services or the Census Bureau. Based on the effectiveness of a variety of safeguards, NASA should consider how to integrate such measures into its current human subjects and privacy protocols in order to protect the confidentiality of information contained in geospatial data.

Once explicit policies, protocols, and procedures are in place for geospatial data, NASA will need to expand its Human Protection Training Program for NASA scientists, administrators, and especially IRB members in order to specifically address geospatial data. These members of the NASA community need to be aware of the inherent risk of disclosing confidential information associated with geospatial data. NASA staff must understand the potential impacts of this risk and the techniques to manage it, in order to effectively protect NASA from damaging political and financial liabilities. To assist both its own staff and other data users, it would be useful for NASA to post online its policies related to confidentiality and geospatial data. In addition, NASA could make web-accessible registries for geo-referenced data requests, related research protocols, Center IRBs, and IRB reviews. This would not only

assist prospective data users, but also help NASA administrators track how NASA data are being utilized, integrated with other datasets, and regulated.

Historically, NASA has had a strong record of protecting the confidentiality of administrative and medical research data. Given the potential of new remote-sensing technology and expanded computer capabilities, NASA must now also anticipate and avert the risk of disclosing personal information from the integration of geospatial data with health and other datasets. By working closely with experts from other agencies and research centers, NASA can learn how to better identify and control such risks. NASA can successfully manage these risks and safeguard confidentiality by expanding its existing policy directives, procedures, and protocols to incorporate new techniques that effectively address the unique aspects of geospatial data.

References[*]

Aboud, J.M., and S. D. Woodcock (2002). Disclosure limitation in longitudinal linked data. In *Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies*, P. Doyle, J.I. Lane, J.J.M. Theeuwes, and L.V. Zayatz, eds. Amsterdam, North Holland: Elsevier, pp. 215-278. http://books.nap.edu /books/0309071801/html/38.html#pagetop (accessed 11 March 2005).

American Statistical Association (ASA), Committee on Privacy and Confidentiality (2003a). *American Statistical Association's Privacy, Confidentiality, and Data Security Website.* http://www.amstat.org/comm/cmtepc/index.cfm?fuseaction=content (accessed 11 March 2005).

American Statistical Association (ASA), Committee on Privacy and Confidentiality (2003b). *Welcome to the American Statistical Association's Privacy, Confidentiality, and Data Security Website.* http://www.amstat.org/comm/cmtepc/index.cfm (accessed 11 March 2005).

Armstrong, M.P., G. Rushton, and D. Zimmerman (1999). Geographically masking health data to preserve confidentiality. *Statistics in Medicine* **18**(5):497-525. http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&list_uids=10209808&dopt=Abstract (accessed 11 March 2005).

Bayer, R., and A.L. Fairchild (2000). Surveillance and privacy. *Public Health and Medicine* **290**:1898-1899.

Blakemore, M. (2002). The potential and perils of remote access. In *Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies*, P. Doyle, J.I. Lane, J.J.M. Theeuwes, and L.V. Zayatz, eds. Amsterdam, North Holland: Elsevier, pp. 315-340.

Buckeridge, D.L., R. Mason, *et al.* (2002). Making health data maps: a case study of a community/university research collaboration. *Social Science & Medicine* **55**(7): 1189-1206. http://www.sciencedirect.com/science/article/B6VBF-46MC8C1-9/2/7c8bbcc5b24e1d682fbb5931d1a1558b (accessed 11 March 2005).

Clough, J.D., D.W. Rowan, and D.E. Nickelson (1999). Keeping our patients' secrets. *Cleveland Clinic Journal of Medicine* **66**(9):554-558.

Computer Matching and Privacy Protection Act of 1988 (1988). Public Law No. 100-503. 100th Congress. As Amended by Public Law No. 101-508. 101st Congress. http://www4.law.cornell.edu/uscode/5/552a.html (accessed 11 March 2005).

Computer Security Act of 1987 (1987). Public Law 100-255, 100th Congress. *Statutes at Large*. 101 Stat. 1724-1730. http://www.house.gov/science_democrats/archive/compsec1.htm (accessed 11 March 2005).

Confidential Information Protection and Statistical Efficiency Act (CIPSEA), E-Government Act of 2002 Title V (2002). Public Law 107-347, 107th Congress. *United States*

[*] Note: Some links given here may require a subscription to an online service.

Statutes at Large. 116 Stat. 2962. December 17, 2002. http://www.aiprp.gouv.qc.ca/publications/pdf/getdoc%5B1%5D.pdf (accessed 11 March 2005).

Cox, L.H. (1996). Protecting confidentiality in small population health and environmental statistics. *Statistics in Medicine* **15**(17-18):1895-1905. http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&list_uids=8888482&dopt=Abstract (accessed 11 March 2005).

Croner, C.M. (2003). Public health GIS and the Internet. *Annual Review of Public Health* **24**:57-82. http://www.cdc.gov/nchs/data/gis/GIS_AND_THE_INTERNET.pdf (accessed 11 March 2005).

de Wolf, V.A. (2003). Issues in accessing and sharing confidential survey and social science data. *Data Science Journal* **2**(17):66-74. http://www.codata.org/codata02/11datapolicy/deWolf/deWolf-paper.pdf (accessed 11 March 2005).

Domingo-Ferrer, J., and V. Torra (2002). A quantitative comparison of disclosure control methods for microdata. In *Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies*, P. Doyle, J.I. Lane, J.J.M. Theeuwes, and L.V. Zayatz, eds. Amsterdam, North Holland: Elsevier, pp. 111-134.

Doyle, P., J.I. Lane, J.J.M. Theeuwes, and L.V. Zayatz, Eds. (2002). *Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies*. Amsterdam, North Holland: Elesevier. http://www.elsevier.com/wps/find/bookdescription.cws_home/622129/description#description (accessed 11 March 2005).

Duncan, G.T. (2003). *Exploring the Tension between Privacy and the Social Benefits of Governmental Databases*. Security, Technology, and Privacy: Shaping a 21st Century Public Information Policy, Georgetown University Law Center, Washington DC.

Duncan, G.T., Jabine, T.B., and V. de Wolf (1993). *Private Lives and Public Policies: Confidentiality and Accessibility of Government Statistics*. Washington DC: National Academy Press.

Duncan, G.T., S.E. Feinberg, R. Krishnan, R. Padman, and S.F. Roehrig (2002). Disclosure limitation methods and information loss for tabular data. In *Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies*, P. Doyle, J.I. Lane, J.J.M. Theeuwes, and L.V. Zayatz, eds. Amsterdam, North Holland: Elsevier, pp. 135-166.

Dunne, T. (2002). Issues in the establishment and management of secure research sites. In *Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies*, P. Doyle, J.I. Lane, J.J.M. Theeuwes, and L.V. Zayatz, eds. Amsterdam, North Holland: Elsevier, pp. 297-314.

E-Government Act of 2002 (2002). HR 2458. Public Law 107-347, 107th Congress. *United States Statutes at Large*. 116 Stat. 2899. http://www.aiprp.gouv.qc.ca/publications/pdf/getdoc%5B1%5D.pdf (accessed 11 March 2005).

Federal Information Security Management Act of 2002, E-Government Act of 2002 Title III (2002). Public Law 107-347, 107th Congress. *United States Statutes at Large*. 116

Stat. 2946. December 17, 2002. http://www.aiprp.gouv.qc.ca/publications/pdf/getdoc%5B1%5D.pdf (accessed 11 March 2005).

Federal Policy for the Protection of Human Subjects (Basic DHHS Policy for Protection of Human Research Subjects, "The Common Rule") (1991a). Revised as of June 18, 1991. *Code of Federal Regulations* Title 45, Part 46 *Protection of Human Subjects, Subpart A.* 56 FR 28003. http://www.hhs.gov/ohrp/references/frcomrul.pdf (accessed 11 March 2005).

Federal Policy for the Protection of Human Subjects (Basic DHHS Policy for Protection of Human Research Subjects, "The Common Rule") (1991b). Revised as of June 18, 1991. *Title 14—Aeronautics and Space, Chapter V—National Aeronautics and Space Administration, Part 1230—Protection of Human Subjects,* 14 CFR Part 1230, *Federal Register* ***56****:117* (18 June 1991): 28019.

Federal Policy for the Protection of Human Subjects (Basic DHHS Policy for Protection of Human Research Subjects, "The Common Rule") (2001). Revised as of November 13, 2001. *Code of Federal Regulations* Title 45, Part 46 *Protection of Human Subjects, Subpart A.* http://www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.htm#subparta (accessed 11 March 2005).

Felso, F., J. Theeuwes, and G.G. Wagner (2002). Disclosure limitation methods in use: Results of survey. In *Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies*, P. Doyle, J.I. Lane, J.J.M. Theeuwes, and L.V. Zayatz, eds. Amsterdam, North Holland: Elsevier, pp. 17-42.

Foley, R. (2002). Assessing the applicability of GIS in a health and social care setting: Planning services for informal careers in East Sussex, England. *Social Science & Medicine* **55**(1):79-96. http://www.sciencedirect.com/science/article/B6VBF-45X00VD-7/2/5cf9d9b437b53e4307fdac1e82c3af7a (accessed 11 March 2005).

Freedom of Information Act (FOIA) (1996). 5 U.S.C. 552, As Amended by Public Law No. 104-231. 104th Congress. *United States Statutes at Large*. 110 Stat. 3048. http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm. (accessed 11 March 2005).

Gabrynowicz, J.I. (2003). Data, information, confidentiality and the legal landscape. Paper presented at the NASA Public Health Applications Program Confidentiality & Geospatial Data Workshop, 16 July 2003, Washington DC.

Giesing, S. (2002). Nonperturbative Disclosure Control Methods for Tabular Data. In *Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies*, P. Doyle, J.I. Lane, J.J.M. Theeuwes, and L.V. Zayatz, eds. Amsterdam, North Holland: Elsevier, pp. 185-214.

Hawala, S. (2000). On the variation of the percent of uniques in a microdata sample and the sample size. Upublished paper, June 2000, cited in *Zip Code Tabulation Area and Confidentiality*, National Center for Health Statistics (NCHS), Centers for Disease Control and Prevention (2003).

Health Insurance Portability and Accountability Act of 1996 (HIPAA) (1996). Public Law 104-191, 104th Congress. *United States Statutes at Large*. 110 Stat. 1936. http://aspe.hhs.gov/admnsimp/pl104191.htm (accessed 11 March 2005).

Hyman, S.E. (2000). The needs for database research and for privacy collide. *American Journal of Psychiatry* **157**(11):1723-1724.

Institute of Medicine (1994). *Health Data in the Information Age*. Committee on Regional Health Data Networks, Division of Health Care Services. Donaldson, M.S. and K.N. Lohr, eds. Washington DC: National Academy Press. http://books.nap.edu/books/0309049954/html/index.html (accessed 11 March 2005).

Institute of Medicine (2002). *Responsible Research: A Systems Approach to Protecting Research Participants*. Committee on Assessing the System for Protecting Human Research Participants, Board on Health Sciences Policy, Institute of Medicine. D. Federman, K. Hanna, and L. Lyman Rodriquez, eds. Washington DC: National Academies Press. http://www.nap.edu/catalog/10508.html; http://www.iom.edu/includes/dbfile.asp?id=4157 (accessed 11 March 2005).

International Statistical Institute (1986). Declaration of professional ethics. *International Statistical Review* **54**:227-242.

Jabine, T.B. (1993a). Procedures for restricted data access. *Journal of Official Statistics* **9**:37-590.

Jabine, T.B. (1993b). Statistical disclosure limitation practices of United States statistical agencies. *Journal of Official Statistics* **9**:427-454.

Kistemann, T., F. Dangendorf, and J. Schweikart (2002). New perspectives on the use of Geographic Information Systems (GIS) in the environmental health sciences. *International Journal of Hygiene and Environmental Health* **205**(3):161-181. http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&list_uids=12040915&dopt=Abstract (accessed 11 March 2005).

Madsen, P. (2003). The ethics of confidentiality. Paper presented at the NASA Public Health Applications Program Confidentiality & Geospatial Data Workshop, 16 July 2003, Washington DC.

Marrett, C. (2002). *Letter from the Chair of the Panel on IRBs, Surveys, and Social Science Research, Committee on National Statistics, to Dr. Daniel Federman, Chair, Committee on Assessing the System for Protecting Human Research Participants, Institute of Medicine, July 1, 2002*. http://www7.nationalacademies.org/cnstat/IRB_Panel.html (accessed 11 March 2005).

Martin, D., and G. Higgs (1997). Population georeferencing in England and Wales: Basic spatial units reconsidered. *Environment and Planning* **29**(2):333-347.

Mayer, T. (2002). *Privacy and Confidentiality Research and the U.S. Census Bureau: Recommendations Based on a Review of the Literature*. Research Report Series, U.S. Bureau of the Census. 1-50, February 7, 2002.

NASA Ames Research Center (2004). Life scientists at Ames: Musculoskeletal research—Robert T. Whalen. *Ames Research Center Website*.

NASA Johnson Space Center (1996). *JSC Institutional Review Board Guidelines for Investigators Proposing Human Research for Space Flight and Related Investigations*. http://jsc-web-pub.jsc.nasa.gov/psrp/docs/JSC20483.pdf (accessed 11 March 2005).

NASA Johnson Space Center (2002). *NASA/JSC Human Research Informed Consent.*

NASA Office of Inspector General (OIG) (2001). *Assessment of the Institutional Review Board for Human Subject Protection at the Johnson Space Center, G-01-002.* Letter to NASA Administrator from David M. Cushing, NASA Inspector General, on October 9, 2001. http://www.hq.nasa.gov/office/oig/hq/inspections/g-01-002.pdf (accessed 11 March 2005).

NASA Policy Directive (NPD) (2002). *Protection of Human Subjects* (NPD 7100.8D). http://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PD_7100_008D_&page_name=main (accessed 11 March 2005).

NASA Policy Directive (NPD) (2003). *Privacy Act—Internal NASA Direction in Furtherance of NASA Regulation (NPD 1382.17F), Revalidated 4/25/03.* http://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PD_1382_017F_&page_name=main (accessed 11 March 2005).

NASA Procedural Requirements (NPR) (1998). *Guidelines for Documentation, Approval, and Dissemination of NASA Scientific and Technical Information (STI).* (NPR 2200.2A, effective September 3, 1998). http://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PR_2200_002A_&page_name=main (accessed 11 March 2005).

NASA Procedural Requirements (NPR) (1999). *Security of Information Technology.* (NPR 2810.1, effective August 16, 1999). http://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PR_2810_0001_&page_name=main (accessed 11 March 2005).

NASA Procedural Requirements (NPR) (2003). *Protection of Human Research Subjects* (NPG 7100.1, effective March 28, 2003). http://nodis3.gsfc.nasa.gov/library/displayDir.cfm?Internal_ID=N_PG_7100_0001_&page_name=main (accessed 11 March 2005).

NASA Public Health Applications Program (PHAP) (2003). *NASA Public Health Applications Program Confidentiality & Geospatial Data Workshop*. Organized by the Socioeconomic Data and Applications Center (SEDAC). Hosted at the National Academies of Science Keck Center, Washington DC, 16 July 2003.

National Center for Health Statistics (NCHS), Centers for Disease Control and Prevention (CDC) (2003). *Zip Code Tabulation Area and Confidentiality*. Joint ECE/Eurostat Work Session on Statistical Data Confidentiality, Conference of European Statisticians, Luxembourg, 7-9 April 2003, sponsored by United Nations Statistical Commission and Economic Commission for Europe and European Commission, Statistical Office of the European Communities (EUROSTAT). http://www.unece.org/stats/documents/2003/04/confidentiality/wp.34.e.pdf (accessed 11 March 2005).

National Institutes of Health (NIH) (2002). Office of Extramural Research. *Certificates of Confidentiality*. http://grants1.nih.gov/grants/policy/coc/ (accessed 11 March 2005).

National Research Council (NRC) (1998). *People and Pixels: Linking Remote Sensing and Social Science.* D. Liverman, E.F. Moran, R.R. Rindfus, and P.C. Stern, eds. Committee on the Human Dimensions of Global Change, Commission on Behavioral and Social Sciences and Education. Washington DC: National Academy Press. http://www.nap.edu/books/0309064082/html/ (accessed 11 March 2005).

National Science Foundation (NSF) (1999). Directorate for Computer and Information Science and Engineering, Division of Experimental and Integrative Activities. *Digital Government Program Announcement NSF 99-103.*

National Science Foundation (NSF) (2003). *NSF Confidentiality Workshop 2003.* http://www.urban.org/nsfpresentations/index.html (accessed 11 March 2005).

O'Dwyer, L.A., and D.L. Burton (1998). Potential meets reality: GIS and public health research in Australia. *Australian and New Zealand Journal of Public Health* **22**(7): 819-823. http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&list_uids=9889450&dopt=Abstract (accessed 11 March 2005).

Olvingson, C., J. Hallberg, T. Timpka, and K. Lindqvist (2003). Ethical issues in public health informatics: Implications for system design when sharing geographic information. *Journal of Biomedical Informatics* **35**(3):178-185. http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&list_uids=12669981&dopt=Abstract (accessed 11 March 2005).

Phillips, R.L., E.L. Kinman, P.G. Schnitzer, E.J. Lindbloom, and B. Ewigman (2000). Using Geographic Information Systems to understand health care access. *Archives of Family Medicine* **9**(10):971-978. http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&list_uids=11115195&dopt=Abstract (accessed 11 March 2005).

President's Commission on Federal Statistics (1971). *Federal Statistics. Vol. I.* Washington DC: U.S. Government Printing Office.

Privacy Act of 1974 (1974). 5 U.S.C. Sec. 552a, as amended, Washington DC: U.S. Department of Justice. http://www.usdoj.gov/foia/privstat.htm (accessed 11 March 2005).

Privacy Act – NASA Regulations (1999). Revised as of January 1, 1999. *Code of Federal Regulations* Title 14, Volume 5, Part 1212. Washington DC: U.S. Government Printing Office. http://www.access.gpo.gov/nara/cfr/waisidx_99/14cfr1212_99.html (accessed 11 March 2005).

Rindfuss, R.R. (2002). Conflicting demands: Confidentiality promises and data availability. *IHDP Update: Newsletter of the International Human Dimensions Programme on Global Environmental Change* (Feb. 2002), pp. 1-4, 8. http://www.ihdp.uni-bonn.de/html/publications/update/update02_02/Update02_02_ art1.html (accessed 11 March 2005).

Rindfuss, R.R., and P.C. Stern (1998). Linking remote sensing and social science: The need and the challenges. *People and Pixels: Linking Remote Sensing and Social Science*. D. Liverman, Moran, E.F., Rindfuss, R.R., and P.C. Stern, eds. Washington DC, National Academy Press**.** pp. 1-27.

Rothstein, M.A. (1998). Genetic privacy and confidentiality: Why they are so hard to protect. *Journal of Law, Medicine & Ethics* **26**: 198-204.

Seastrom, M.M. (2002). Licensing. In *Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies*, P. Doyle, J. Lane, J.J.M. Theeuwes, and L. Zayatz, eds. Amsterdam, North Holland: Elsevier, pp. 279-296.

Steel, P., and J. Sperling (2001). *The Impact of Multiple Geographies and Geographic Detail on Disclosure Risk: Interactions between Census Tract and ZIP Code Tabulation Geography*. U.S. Census Bureau, unpublished monograph. www.census.gov/srd/sdc/steel.sperling.2001.pdf (accessed 11 March 2005).

USA PATRIOT ACT: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (2001). H.R. 3162. Public Law 107-56, 107th Congress. http://www.epic.org/privacy/terrorism/hr3162.pdf (accessed 11 March 2005)

U.S. Census Bureau (US Census), The Center for Economic Studies (CES) (2003). *Carnegie Mellon Research Data Center*. April 10, 2003. http://www.ces.census.gov/ces.php/home (accessed 11 March 2005).

U.S. Congress. House. Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform (2003). *Geographic Information Systems: Challenges to Effective Data Sharing.* Testimony by Linda D. Koontz, Director of Information Management Issues, U.S. General Accounting Office. Washington DC, June 10, 2003. GAO-03-874T. http://www.gao.gov/new.items/d03874t.pdf (accessed 11 March 2005).

U.S. Congress, Office of Technology Assessment (OTA) (1986). *Federal Government Information Technology: Electronic Record Systems and Individual Privacy. OTA-CIT-296*. Washington DC: U.S. Government Printing Office, June 1986. http://www.wws.princeton.edu/cgi-bin/byteserv.prl/~ota/disk2/1986/8606/_8606.PDF (accessed 11 March 2005).

U.S. Department of Commerce (DOC), National Bureau of Standards (NBS) (1975). *Computer Security Guidelines for Implementing the Privacy Act of 1974*. Federal Information Processing Standards Publication, FIPS PUB 41. Washington DC: Government Printing Office, May 30, 1975. http://www.itl.nist.gov/fipspubs/withdraw.htm (accessed 11 March 2005).

U.S. Department of Energy (US DOE), Office of Health and Environmental Research. (1996). NASA's new human subjects policy. *Protecting Human Subjects*, Fall 1996. http://www.er.doe.gov/production/ober/humsubj/fall96/fall9605.html (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS) Centers for Disease Control and Prevention (CDC) and the Agency for Toxic Substances and Disease Registry (ATSDR) (2003). *CDC/ATSDR Procedures for Protection of Human Research Participants: 2003.* http://www.cdc.gov/od/ads/procphrp.pdf. (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS) Centers for Disease Control and Prevention (CDC) and Council of State and Territorial Epidemiologists (CSTE) (2003 Draft). *CDC-CSTE Intergovernmental Data Release Guidelines Working Group (DRGWG) Report: CDC-ATSDR-CSTE Data Release Guidelines for Re-release State Data.* Draft report for soliciting input and feedback (drgwg report ver 6-2.doc).

U.S. Department of Health and Human Services (US DHHS) Centers for Disease Control and Prevention (CDC), Office for Science Policy and Technology Transfer (OSPTT) (2004). *Human Subjects Research.* http://www.cdc.gov/od/ads/hsr2.htm (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS), National Institutes of Health (NIH) (1995). Revised 2 March 1995. *Guidelines for the Conduct of Research Involving Human Subjects at the National Institutes of Health*. http://www.nihtraining.com/ohsrsite/guidelines/graybook.html (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS), National Institutes of Health (NIH) (2003a). *Certificates of Confidentiality Kiosk.* http://grants.nih.gov/grants/policy/coc/index.htm (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS), National Institutes of Health (NIH) (2003b). *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule*. http://privacyruleandresearch.nih.gov/pr_02.asp (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS), Office of Civil Rights (OCR) (2002). *Standards for Privacy of Individually Identifiable Health Information (The Privacy Rule), Final Modifications. Federal Register* 67 (August 14, 2002). *Code of Federal Regulations*, Title 45, Parts 160 and 164. http://www.hhs.gov/ocr/hipaa/finalreg.html (accessed 11 March 2005); http://privacyruleandresearch.nih.gov/ (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS), Office for Civil Rights (OCR) (2003). *Website on Medical Privacy- National Standards to Protect the Privacy of Personal Health Information*. http://www.hhs.gov/ocr/hipaa (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS). Office for Human Research Protections (OHRP) (2000a). *Human Subject Regulations Decision Charts*. http://www.hhs.gov/ohrp/humansubjects/guidance/decisioncharts.htm (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS). Office for Human Research Protections (OHRP) (2000b). *Informed Consent Checklist.* http://www.hhs.gov/ohrp/humansubjects/assurance/consentckls.htm (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS). Office for Human Research Protections (OHRP) (2002). *Human Research Protections Database*. U.S. Department of Health and Human Services (US DHHS).

U.S. Department of Health and Human Services (US DHHS). Office for Human Research Protections (OHRP) (2003a). *Assurances and IRB Registration.* http://www.hhs.gov/ohrp/assurances/assurances_index.html (accessed 11 March 2005); http://www.hhs.gov/ohrp/assurances/ (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS). Office for Human Research Protections (OHRP) (2003b). *Federalwide Assurance (FWA).* http://www.hhs.gov/ohrp/humansubjects/assurance/filasurt.htm (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS). Office for Human Research Protections (OHRP) (2003c). *Institutional Review Board (IRB) Registration.* http://www.hhs.gov/ohrp/assurances (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS). Office for Human Research Protections (OHRP) (2003d). *Policy Guidance.* http://www.hhs.gov/ohrp/policy/ (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS). Office for Human Research Protections (OHRP) (2004). *General OHRP Information*. http://www.hhs.gov/ohrp/ (accessed 11 March 2005).

U.S. Department of Justice (US DOJ). Office of Information and Privacy (2002, last updated*). FOIA Update (1979-2000*). http://www.usdoj.gov/oip/foi-upd.htm (accessed 11 March 2005).

U.S. General Accounting Office (US GAO), Health Services Quality and Public Health Issues (1999). *Medical Records Privacy: Access Needed for Health Research, But Oversight of Privacy Protections is Limited. (Report to Congress, 24 February 1999, GAO/HEHS-99-55).* http://www.epic.org/privacy/medical/gao-medical-privacy-399.pdf (accessed 11 March 2005).

U.S. General Accounting Office (US GAO) (2001). *Record Linkage and Privacy: Issues in Creating New Federal Research and Statistical Information.* GAO-01-126SP. Washington DC, April 2001. http://www.gao.gov/new.items/d01126sp.pdf (accessed 11 March 2005).

U.S. Office of Management and Budget (US OMB) (1989). Privacy Act of 1974; Final guidance interpreting the provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988. *Federal Register* **54**:116 (1989): 25818-25829. http://www.dod.mil/privacy/1975OMB_PAGuide/jun1989.pdf (accessed 11 March 2005).

U.S. Office of Management and Budget (US OMB) (1990). *Circular No. A-16 Revised: Coordination of Surveying, Mapping, and Related Spatial Data Activities.* http://clinton4.nara.gov/textonly/OMB/circulars/a016/a016.html (accessed 11 March 2005).

U.S. Office of Management and Budget (US OMB) (2000a). Revision of Circular No. A-130, Transmittal No. 4: Management of Federal Information Resources. *Federal Register **65***:239, 12 December 2000. http://www.ogc.doc.gov/ogc/contracts/cld/ecomm/65fr77677.html (accessed 11 March 2005).

U.S. Office of Management and Budget (US OMB) (2000b). *Memorandum for Heads of Executive Departments and Agencies: Guidance on Inter-Agency Sharing of Personal Data--Protecting Personal Privacy* (M-01-05), 20 December 2000. http://www.whitehouse.gov/omb/memoranda/m01-05.html (accessed 11 March 2005).

U.S. Office of Management and Budget (US OMB) (2002). *Circular No. A-16 Revised: Coordination of Geographic Information and Related Spatial Data Activities.* http://www.whitehouse.gov/omb/circulars/a016/text/a016_rev.html (accessed 11 March 2005).

U.S. Office of Management and Budget (US OMB) (2003). *Memorandum for Heads of Executive Departments and Agencies: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (M-03-22), 26 September 2003. http://www.whitehouse.gov/omb/memoranda/m03-22.html (accessed 11 March 2005).

U.S. Office of Management and Budget (US OMB). Federal Committee on Statistical Methodology (FCSM) (1994). *Report on Statistic Disclosure Limitation Methodology: Statistical Policy Working Paper 22*. http://www.fcsm.gov/working-papers/spwp22.html (accessed 11 March 2005).

U.S. Office of Management and Budget (US OMB). Federal Committee on Statistical Methodology (FCSM), Confidentiality and Data Access Committee (CDAC) (1999). *Checklist on Disclosure Potential of Proposed Data Releases.* http://www.fcsm.gov/committees/cdac/cdac.html (accessed 11 March 2005).

U.S. Office of Management and Budget (US OMB). Federal Committee on Statistical Methodology (FCSM), Confidentiality and Data Access Committee (CDAC) (2002). *Restricted Access Procedures: Confidentiality and Data Access Committee.* www.fcsm.gov/committees/cdac/cdacra9.pdf (accessed 11 March 2005).

U.S. Office of Management and Budget (US OMB). Federal Committee on Statistical Methodology (FCSM), Confidentiality and Data Access Committee (CDAC) (2004). *About CDAC.* Confidentiality and Data Access Committee (CDAC) Website. http://www.fcsm.gov/committees/cdac/about.html (accessed 11 March 2005).

U.S. President, W.J. Clinton. Memorandum for the Vice President, the Heads of Executive Departments, and Agencies (1994.) *Review of Federal policy for the Protection of Human Subjects*, February 17, 1994. http://www.hhs.gov/ohrp/humansubjects/guidance/hsdc94feb.htm (accessed 11 March 2005).

U.S. President's Advisory Committee on Human Radiation Experiments (ACHRE) (1995). *Final Report of the Advisory Committee on Human Radiation Experiments.* Washington DC: Government Printing Office (stock number 061-000-00-848-9). http://tis.eh.doe.gov/ohre/roadmap/achre/chap18.html (accessed 11 March 2005).

Warren, S.D., and L.D. Brandeis (1890). The right to privacy. *Harvard Law Review* **IV**(5).

Appendix I: NASA Public Health Applications Program Confidentiality and Geospatial Data Workshop

16 July 2003
National Academy of Sciences
500 Fifth Street, NW, Room 201
Washington DC 20001

Agenda

9:30 – 10:10 Welcome and Participant Introductions

Dr. Roberta Balstad Miller, Director, CIESIN, Columbia University

Dr. Robert A. Venezia, Program Manager for Public Health Applications, NASA

10:10 – 10:30 Overview of Issues

Dr. Deborah Balk, Lead SEDAC Project Scientist, CIESIN, Columbia University

10:30 – 10:45 Break

10:45 – 12:30 Confidentiality Issues When Using Geospatial Data for Public Health Applications, *Moderator, Dr. Roberta Balstad Miller, CIESIN*

The Agency Perspective, Dr. Thomas Baerwald, Senior Science Advisor, Division of Behavioral and Cognitive Sciences, National Science Foundation

The Researcher Perspective, Dr. Ronald Rindfuss, Faculty Fellow, Carolina Population Center, University of North Carolina at Chapel Hill.

The Legal Perspective, Prof. Joanne Gabrynowicz, Director, University of Mississippi National Remote Sensing and Space Law Center

The Ethical Perspective, Dr. Peter Madsen, Director, Center for Advancement of Applied Ethics, Carnegie Mellon University

The Commercial Perspective, Mr. Jerry Garegnani, Staff Officer, ESRI, Inc.

12:30 – 1:30 Lunch: Available in Cafeteria on 3rd Floor (one flight up)

1:30 – 3:00 **Government Agency Panel Discussion**, *Moderator, Dr. Robert Venezia, NASA*

Questions to be addressed:
1) When have problems related to confidentiality arisen?
2) How have you or your agency overcome these problems?
3) What barriers remain?
4) What would be your agency requirements if sharing data with other agencies?
5) Does your agency have different requirements when funding projects vs. sharing data?

Panel Members:
1) Dr. Stephen Guptill, Senior Research Physical Scientist, U. S. Geological Survey
2) Dr. C. Virginia Lee, Medical Officer, OAA, Agency for Toxic Substances and Disease Registries (ATSDR), CDC
3) Mr. Mario Merlino, Director, Office of Policy and Planning, Division of Financial and Strategic Management, New York City Department of Health
4) Mr. Philip M. Steel, Disclosure Avoidance Staff, Statistical Research Division, US Census Bureau
5) Dr. Alvan Zarate, Confidentiality Officer, National Center for Health Statistics (NCHS), CDC
6) Dr. Rebecca Clark, Health Scientist Administrator, Demographic and Behavioral Sciences Branch, National Institute of Child Health and Development (NICHD)

3:15 – 3:30 **Break**

3:30 – 4:45 **Researcher Panel Discussion**, *Moderator, Dr. Charles Croner, NCHS*

Questions to be addressed:
1) What key questions can be answered with the integration of RS and socioeconomic data?
2) How does the use of RS data potentially compromise the confidentiality of demographic, socioeconomic, and health data or related research results?
3) What approaches have succeeded or failed to preserve confidentiality in order to make data accessible to researchers, policymakers, or the public?
4) In what form or with what restrictions do you or your institution release data?
5) Do you or your institution have a data preservation plan?

Panel Members:
1) Ms. Livia Montana, GIS Specialist, Demographic and Health Surveys, ORC Macro
2) Dr. Gregory Gurri Glass, Professor, Molecular Microbiology and Immunology, Johns Hopkins Bloomberg School of Public Health
3) Dr. Myron Gutmann, Director, Inter-university Consortium for Political and Social Research (ICSPR)
4) Dr. Charles Taylor, Professor, Department of Organismic Biology, Ecology, and Evolution, UCLA

4:45 – 5:30 **Next Steps**, *Moderator, Dr. Deborah Balk, CIESIN*

NASA Public Health Applications Program
CONFIDENTIALITY & GEOSPATIAL DATA WORKSHOP
Participant List
16 July 2003

Tom Baerwald, National Science Foundation
Deborah Balk, CIESIN, Columbia University
Rebecca Clark, NICHD/NIH
Charles Croner, NCHS/CDC
Robert Downs, CIESIN, Columbia University
Julie Esanu, National Academies
Fazlay Faruque, University of Mississippi Medical Center
Debbie Fendley, NASA SSC
Richard Finley, University of Mississippi Medical Center
Joanne Gabrynowicz, University of Mississippi
Jerry Garegnani, ESRI, Inc.
Gregory Gurri Glass, Johns Hopkins Bloomberg School of Public Health
Rob Gutro, NASA Goddard
Meredith Golden, CIESIN, Columbia University
Stephen Guptill, U. S. Geological Survey
Myron Gutmann, ICSPR
Richard Kiang, NASA
Daniel Kimes, NASA
C. Virginia Lee, ATSDR/CDC
Elissa Levine, NASA
Peter Madsen, Carnegie Mellon University
Nancy Maynard, NASA
Mario Merlino, New York City Department of Health
Roberta Balstad Miller, CIESIN, Columbia University
Livia Montana, DHS/ORC Macro
Cynthia O'Carroll, NASA Goddard
Kent Davis-Packard, CIESIN, Columbia University
Ronald Rindfuss, UNC-Chapel Hill
Robert E. Ryan, NASA SSC
J. Marshall Shepherd, NASA HQ
Philip M. Steel, US Census Bureau
Charles Taylor, UCLA
Elvia Thompson, NASA HQ
Sidey Timmins, SSAI, Inc
Compton J. Tucker, NASA
Asad Ullah, SSAI Inc.
Lauren Underwood, NASA SSC
Robert A. Venezia, NASA
Gilberto Vincente, George Mason University
Rita Aissi-Wespi, DSTI Inc.
Boris Yurchak, NASA
Vicki Zanoni, NASA SSC
Alvan Zarate, NCHS/CDC

Appendix II: American Statistical Association's Privacy, Confidentiality, and Data Security Website

http://www.amstat.org/comm/cmtepc/index.cfm?fuseaction=content

I. Privacy, Confidentiality, and Data Dissemination Guidelines for Government Agencies and International Organizations

B. United States Federal Agencies and States

2. Individual Executive Branch Departments

a. Commerce

153 - U.S. Census Bureau, Center for Economic Studies (CES) Privacy and Policy Statements' "Protection of Confidentiality Information," content (R)
sponsor (G)
A statement of Title 13, sections 9 and 214.

154 - U.S. Census, Statistical Research Division's "Privacy and Confidentiality Research and the U.S. Census Bureau: Recommendations Based on a Review of the Literature," Research Report Series, Survey Methodology #2002-01 (2002, Thomas Mayer)
content (D), (R)
sponsor (G)
"This paper explores a number of issues regarding privacy concerns and attitudes, confidentiality beliefs, and their relationship to the functions of the U.S. Census Bureau."

155 - U.S. Census' Statistical Disclosure Control (SDC) content (R), (D)
sponsor (G)
"This page provides links and conventional references to much of the research sponsored by the U.S. Census Bureau in the areas of statistical disclosure control, confidentiality, and disclosure limitation."

b. Education

220 - National Center for Education Statistics, Statistical Standard 4-2, "Maintaining Confidentiality"
content (D)
sponsor (G)
The purpose of this standard is "to protect the confidentiality of NCES data that contain

information about individuals (individually identifiable information). For this reason, staff must be cognizant of the requirements of the law and must monitor the confidentiality of individually identifiable information in their daily activities and in the release of information to the public."

221 - National Center for Education Statistics, (NCES) Statistical Standards content (D) sponsor (G)
Includes standards on documentation and dissemination of data.

222 - Protecting the Privacy of Student Records: Guidelines for Education Agencies (1997, Oona Cheung, Barbara Clements, and Ellen Pechman, U.S. Department of Education, National Center for Education Statistics.) content (D) sponsor (G)
This document addresses the need for the members of the education community to understand their legal responsibilities and to develop procedures to maintain the privacy of student records.

156 - U.S. Department of Education, "Protection of Human Subjects in Research", content (D), (R) sponsor (G)
A set of links in the following categories: General Information; Regulations Governing the Protection of Human Subjects in Research; Guidance and Educational Materials, and Assurance Information and Other.

157 - National Center for Education Statistics, Restricted Use Data Procedures Manual content (R), (D) sponsor (G)
An on-line manual reviewing laws, licensing procedures, data security, and on-site inspections.

c. Energy

158 - U. S. Department of Energy's "Human Subjects Regulations, Orders, Policy Statements, and Legislation," content (R), (D)

sponsor (G)
An index of links to Dept of Energy documents.

159 - Energy Information Administration's Standards for Statistical Activities, U.S. Department of Energy
content (R), (D)
sponsor (G)
Two EIA standards of particular interest are: 2002-21- Data Protection and Accessibility, and 2002-22 Non-disclosure of Company Identifiable Data in Aggregate Cells. Also of note are the Supplemental materials for Standard 2002-22, "Guidelines for Implementation of a Disclosure Limitation Rule," which explains in how to apply the pq rule.

d. Health and Human Services

160 - U.S. Department of Health and Human Services Administrative Simplification website
content (R)
sponsor (G)
The Health Information Portability and Accountability Act of 1996 (HIPAA) included an "Administrative Simplification" provision requiring the Department of Health and Human Services to establish national standards to protect the privacy of personal health information maintained in electronic form, and to develop regulations for the adoption and maintenance of these standards. This site provides links that describe the agency's activities and progress in implementing these requirements.

Direct links from this site include:

Office of Civil Right's "Medical Privacy - National Standards to Protect the Privacy of Personal Health Information,"
content (R), sponsor (G)
This link has the latest/ final changes to the HIPAA and other similar rules.

161 - National Institutes of Health, Notice for the Required Education in the Protection of Human Research Participants
content (R), (D)

sponsor (G)
"Beginning on October 1, 2000, the NIH will require education on the protection of human research participants for all investigators submitting NIH applications for grants or proposals for contracts or receiving new or non-competing awards for research involving human subjects."

162 - National Institutes of Health's Notice "Revised Policy for IRB Review of Human Subjects Protocols in Grant Applications"
content (R)
sponsor (G)
Announcement that grants submitted after June/July 2000 must have IRB approval at time of submission or within 60 days of approval.

163 - U.S. Department of Health and Human Services, Office for Human Research Protection's (OHRP) Main page
content (D), (R)
sponsor (G)
General information about the OHRP with links to the site's 5 major content areas: IRB Regulations and Assurances, Policy Guidelines, Compliance and Oversight, Educational Materials, and Workshops.

Specific links from the U.S. Department of Health and Human Services, Office for Human Research Protection's Main Page

IRB Guidebook,
content (R), (D), sponsor (G)
Online Guidebook with information on ordering videotape series: "Protecting Human Subjects."

IRB Registration and Assurance Filing Documents,
content (R), (D), sponsor (G)
The site contains: "information, instructions, and the necessary form(s) to: 1) register an Institutional Review Board (IRB) or an Independent Ethics Committee (IEC), 2) prepare an application for a Federalwide Assurance (FWA) for the Protection of Human Subjects in Research or obtain information about other types of

Assurances or approval of an Assurance, or 3) to initiate the Quality Improvement process."

Code of Federal Regulations, Title 45, Part 46, the "Common Rule" (revised Nov 2001),
content (R), sponsor (G)
Federal code governing research conducted on human subjects.

"Frequently Sought Information" of the OHRP,
content (R), (D), sponsor (G)
A list of questions and answers regarding IRB and assurance issues.

164 - National Center for Health Statistics, NCHS Public-use Data Files and Documentation
content (D), (R)
sponsor (G)
The site's information is specific to NCHS datasets. Links of interest include "Data Use Restrictions" and "Data Release."

e. Justice

165 - U.S. Department of Justice's "Summary of Human Subject Protection Issues Related to Large Sample Surveys," (June 2001)
content (R) (D)
sponsor (G)
This site discusses ways of ensuring ethical compliance with the Common Rule in the conduct of large sample surveys.
(text version of the Report)
(pdf version of the Report)

f. Labor

239 - U.S. Department of Labor, Bureau of Labor Statistics, " Bureau of Labor Statistics Data Integrity Guidelines"
content (R), (D)
sponsor (G)
"The following guidelines must be followed by all Bureau of Labor Statistics (BLS) program offices and BLS employees to ensure the integrity of information maintained and disseminated by the BLS. Office of

Management and Budget (OMB) information quality guidelines define 'Integrity' as the security of information-protection of the information from unauthorized access or revision, to ensure that the information is not compromised through corruption or falsification." Topic areas include: the Confidential nature of BLS records, Data collection, Procedures for safeguarding confidential information, Dissemination of news and data releases, and Data security.

g. Treasury

240 - U.S. Bureau of the Treasury, Office of Tax Policy, Report to The Congress on Scope and Use of Taxpayer Confidentiality Provisions; Volume I: Study of General Provisions, October 2000
content (R), (D)
sponsor (G)
"Section 3802 of the Internal Revenue Service Restructuring and Reform Act of 1998 ("RRA 1998") requires the Secretary of the Treasury and the Joint Committee on Taxation (the "JCT") to conduct separate studies of the scope and use of provisions regarding taxpayer confidentiality and to report the findings of such study, together with any recommendations deemed appropriate to Congress. The staff of the Joint Committee on Taxation (the "JCT staff") published its report on January 28, 2000.

.

Appendix III: Related Activities

Committees, Panels, and Workgroups

American Statistical Association's (ASA) Committee on Privacy and Confidentiality

http://www.amstat.org/comm/cmtepc/

Purpose:

- To review legislation in the area of privacy and confidentiality and to monitor the application of privacy and confidentiality laws, regulations, and guidelines.
- To communicate to the ASA members activity in privacy and confidentiality relevant to statistics.
- To provide an early warning system to the Board of Directors on privacy and confidentiality matters that may affect statisticians.
- To serve as a focal point within ASA for contact with other associations on matters related to privacy and confidentiality.
- To monitor and encourage new technical developments related to privacy and confidentiality of data collected or used for statistical purposes.
- To develop appropriate liaison with Congressional Committees and Federal agencies on matters relating to privacy and confidentiality.
- To represent ASA in Congressional hearings on privacy and confidentiality, at the request of the Board of Directors.
- To make suggestions to the Board of Directors for needed study and action in the area of privacy and confidentiality.

Chair: Alvan Zarate, National Center for Health Statistics

Website includes: Guidelines for government agencies and international organizations; Statistical Methods for privacy, confidentiality, and disclosure limitations; Human Subjects Protection in Research and Institutional Review Boards (IRBs); Health Care, Bioethics, and Personal Health Information; Topics in Education; Topics in Finance; Ethics, Principles, and Standards; Legal and regulatory sites; and Training opportunities.

CDC-CSTE Intergovernmental Data Release Guidelines Working Group (DRGWG)

Convened by the Centers for Disease Control and Prevention (CDC) and the Council of State and Territorial Epidemiologists (CSTE), February 2001.

Purpose: To revise the notifiable disease data release procedure and to address the need for uniformity of data re-release, across CDC programs

Membership: ATSDR, AEP, NCBDDD, NCCDPHP, NCEH, NCHS, NCHSTP, NCID, NCIPC, NIOSH, NIP, PHPPO, OD, and CSTE (5 members)
Chairs: RA Jajosky, CDC Epidemiology Program Office and S. Macdonald, CSTE

Report: *CDC-CSTE Intergovernmental Data Release Guidelines Working Group (DRGWG) Report: CDC-ATSDR-CSTE Data Release Guidelines for Re-release State Data* (CDC and CSTE, draft 2003).

Confidentiality and Data Access Committee (CDAC)
http://www.fcsm.gov/committees/cdac/cdac.html
http://www.fcsm.gov/committees/cdac/cdacpaper.pdf

Convened by The Office of Management and Budget's (OMB) Federal Committee on Statistical Methodology (FCSM) as the Interagency Confidentiality and Data Access Group (ICDAG) in 1996 (recommended in FCSM's Statistical Policy Working Paper #22 Report on Statistical Disclosure Limitation Methodology, May 1994)

Purpose: To serve as a forum for staff members of statistical agencies "to promote cooperation and sharing of information concerning data access issues and statistical disclosure methods among Federal agencies."

Chair: Steve Cohen, Bureau of Labor Statistics
Vice-Chair Philip Steel, US Census Bureau

Department of Health and Human Services (DHSS) Secretary's Advisory Committee on Human Research Protections (SACHRP)
http://ohrp.osophs.dhhs.gov/sachrp/sachrp.htm
http://ohrp.osophs.dhhs.gov/sachrp/mtgings/mtg07-03/minjul03.htm

Replaced the National Human Research Protections Advisory Committee (NHRPAC) in October 2002 (first Inaugural Meeting in July 2003)

Purpose: "To advise the Secretary of DHHS on all matters related to human subjects with a particular emphasis on special populations including children, neonates, decisionally impaired individuals, and prisoners. SACHRP also is mandated to address… research with individually identified samples, data, or information…" (Inaugural Meeting, July 22, 2003)

Chair: Ernest Prentice, University of Nebraska Medical Center

Institute of Medicine (IOM) Committee on Assessing the System for the Protection of Human Research Participants
http://www4.nationalacademies.org/cp.nsf/Projects+_by+_PIN/HSPX-H-00-05-A

Convened by the Institute of Medicine September 2001, duration 24 months.

Purpose: To conduct a two-phase study to address 1) accreditation standards for Human Research Participant Protection Programs (HRPPPs), 2) the overall structure and function of HRPPPs, including but not restricted to Institutional Review Boards, and 3) criteria for evaluating the performance of HRPPPs.

Reports: *Preserving Public Trust: Accreditation and Human Research Participant Protection Programs* (IOM, April 2001)
Responsible Research: A Systems Approach to Protecting Research Participants (IOM, 2002)

National Bioethics Advisory Committee (NBAC)
http://www.georgetown.edu/research/nrcbl/nbac/

Established in 1995 by President Clinton by Executive Order 12975, Protection of Human Research Subjects and Creation of National Bioethics Advisory Commission. Charter expired on October 3, 2001 and not renewed.

Purpose: 1) To provide advice and make recommendations to the National Science and Technology Council and other government entities regarding bioethical issues related to research on human biology and behavior; 2) To identify broad principles to govern ethical conduct of research; 3) To respond to requests from the National Science and Technology Council, Congress, and the public.

Reports: http://www.georgetown.edu/research/nrcbl/nbac/pubs.html

(See also President's Council on Bioethics, established November 28, 2001, Executive Order 13237, http://www.bioethics.gov/)

National Human Research Protections Advisory Committee (NHRPAC's) Social and Behavioral Science Working Group (SBSWG) (see American Sociological Association)
http://www.asanet.org/public/humanresearch/

Purpose: To develop guidelines for the review of social and behavioral science research by institutional review boards (IRBs) addressing issues such as the review of public-use data files, risk and harm, and third parties. (Although DHHS' NHRPAC was disbanded in 2002 and replaced with SACHRP, the SBSWG continues its work independently of the SACHRP.)
Roster: http://ohrp.osophs.dhhs.gov/hnrpac/wrksanb.htm

Staff: Paula Skedsvold, American Sociological Association

Office of Science and Technology Policy (OSTP), Committee on Science, Human Subjects Research Subcommittee (HSRS)

Purpose: To provide advice about interdepartmental issues in protection of human participants to OSTP's Committee on Science and to the departments and agencies that promulgate the "Common Rule"

Chair: OHRP's Director (Bernard A. Schwetz, OHRP Acting-Director)

Panel on Confidentiality and Data Access

Convened by the Committee on National Statistics (CNSTAT) of the National Academy of Sciences-National Research Council and the Social Science Research Council (SSRC) in

1989. Supported by the National Science Foundation, the Bureau of the Census, the Bureau of Labor Statistics, the IRS Statistics of Income Division, The National Institute on Aging, the National Center for Education Statistics, and other Federal agencies

Goal: To provide recommendations to Federal agencies to aid them in their stewardship of data for public decisions and research

Members: Experts in the fields of ethics, privacy, respondent issues, public policy, legislation, history of the Federal statistical system, and statistics

Chair: George T. Duncan, Carnegie Mellon University

Report: *Private Lives and Public Policies: Confidentiality and Accessibility of Government Statistics* (NRC and SSRC, 1993).

Panel on Confidential Data Access for Research Purposes
http://www7.nationalacademies.org/cnstat/Data_Access_Panel.html

Convened by the Committee on National Statistics (CNSTAT), National Research Council, January 2003

Purpose: To follow-up topics discussed in October 1999 CNSTAT Workshop: to study and make recommendations about how microdata (especially longitudinal microdata) can best be made available to researchers while protecting respondent confidentiality

Chair: Eleanor Singer, Institute for Social Research, University of Michigan

Panel on Institutional Review Boards, Surveys, and Social Science Research

Convened by the Committee on National Statistics (CNSTAT) and the Board on Behavioral, Cognitive, and Sensory Sciences (BCSSE), National Academies' National Research Council, June 2001

Purpose: To examine the structure, function, and performance of the IRB system as it relates to social, behavioral, and economic sciences (SBES) research and to recommend research and practice to improve the system

Chair: Cora B. Marrett, University of Wisconsin

Report: *Protecting Participants and Facilitating Social and Behavioral Sciences Research* (NRC, 2003)

Privacy, Confidentiality and Data Sharing Workgroup (PCDS)
http://www.cdc.gov/nchs/otheract/phdsc/pcdswkg.htm

Convened on December 9, 2002 by the Public Health Data Standards Consortium (PHDSC)
http://www.cdc.gov/nchs/otheract/phdsc/phdsc.htm

Purpose: To focus on issues of patient privacy and confidentiality while allowing the necessary data sharing for public health and health services research purposes: 1) represent public health and health services research interests on privacy issues, including attending key meetings, 2) provide education, partnerships, and collaboration at the local, state, and national levels, 3) to partner with Standard Development Organizations (SDO), professional organizations, consumer organizations, and others to obtain guidance and clarification … about privacy, confidentiality, and data sharing issues, 4) to collaborate with the Health Care Services Data Reporting Work Group and other Consortium workgroups to develop related projects that promote data standardization, 5) to conduct outreach, and 6) to collect data from Consortium members who have difficulty obtaining protected health information from covered entities because of the privacy regulation.

Chair: Johnathan Lawniczak, AcademyHealth

Conferences and Workshops

Conference on Disclosure Limitation Approaches and Data Access

Convened by the National Research Council and The Social Science Research Council Panel on Confidentiality and Data Access.

March 1991.

Commissioned papers available in a special issue of the Journal of Official Statistics, 1993.

Confidentiality, Disclosure and Data Access Conference

http://www.census.gov/srd/sdc/bookprogramflat.pdf

Convened by the U.S, Census Bureau, U.S. Bureau of Labor Statistics, American Statistical Association (ASA) Committee on Privacy and Confidentiality, Federal Committee on Statistical Methodology, Government Statistics Section of the ASA, Washington Statistical Society, and the Council of Professional Associations on Federal Statistics.

January 7-9, 2002 at the Bureau of Labor Statistics in Washington DC

Goal: To highlight the progress that statistical agencies are making in addressing the challenges of protecting confidentiality (avoiding disclosure), but maximizing access, from both a theoretical and practical standpoint. To review and discuss the new state-of-the-art techniques described by the authors of a new book: *Confidentiality, Disclosure, and Data Access: Theory and Practical Applications for Statistical Agencies*, edited by P. Doyle, J. Lane, J. Theeuwes, and L. Zayatz and published in 2002.

NSF Confidentiality Workshop

http://www.urban.org/nsfpresentations/index.html

Convened by the National Science Foundation and organized by the Urban Institute.

May 12-13, 2003.

Goal: Bring together a small group of 25 researchers to jointly flesh out the basic research agenda for an identified set of broad-ranging confidentiality issues covering a variety of disciplines

Sessions:

- Rethinking the Conceptual Framework
- New Technological Approaches
- Understanding the Data Dissemination Context
- Confidentiality Issues with GeoSpatial Data

The Longitudinal Retirement History Workshop
http://books.nap.edu/books/0309047439/html/245.html#pagetop

Convened by the Committee on National Statistics and the Social Science Research Council at the request of the National Institute on Aging (NIA) and the Census Bureau.

September 18-19, 1987.

Goals: Include understanding the problems and issues in protecting confidential data, disclosure limitation practices, methods to access confidential data for research

Chaired by Jerry A. Hausman

Workshop on Confidentiality of and Access to Doctorate Records
http://books.nap.edu/books/0309047439/html/246.html#pagetop

Convened by the Committee on National Statistics (CNSTAT) and the Social Science Research Council (SSRC)

November 4-5, 1988.

Purpose: To determine if and how mechanisms for allowing greater researcher access to data from the Doctorate Records File and the Survey of Doctorate Records could be developed without compromising the confidentiality of the data. To identify issues for the Panel on Confidentiality and Data Access to address.

Chair: George T. Duncan

Workshop on Confidentiality of and Access to National Center for Education Statistics Data
http://books.nap.edu/books/0309047439/html/246.html#pagetop

Convened by the Panel on Confidentiality and Data Access, Committee on National Statistics (CNSTAT) of the National Academy of Sciences-National Research Council and the Social Science Research Council (SSRC).

January 1991.

Purpose: To investigate confidentiality and access issues as they apply to the National Center for Education Statistics (NCES) and to obtain information for the Panel's deliberations.

Chair: William M. Mason

Workshop on Confidentiality of and Access to Data Research Files
http://www7.nationalacademies.org/cnstat/Workshop_Confidentiality.html

Convened by The Committee on National Statistics (CNSTAT), Division of Behavioral and Social Sciences and Education within The National Academies, and in consultation with the Institute of Medicine (IOM).

October 14-15, 1999

Participants: Data producers from Federal agencies and research organizations; Data users, including academic researchers; and Experts in statistical disclosure limitation techniques, confidentiality policies, and administrative and legal procedures

Chair: Norman Bradburn, National Opinion Research Center

Goals accomplished:

- Reviewed current practices and concerns of Federal agencies and other data producing organizations;
- Reviewed the types of research that are enhanced, or only made possible, using linked longitudinal data;
- Provided an overview of administrative arrangements to preserve confidentiality;
- Identified ways to foster data accessibility in secondary analysis; and
- Assessed the utility of statistical methods for limiting disclosure risk.

Workshop on Data Access and Confidentiality—Access to Research Data: Assessing Risks and Opportunities
http://www7.nationalacademies.org/cnstat/Data_Access_Panel.html
http://www4.nas.edu/webcr.nsf/MeetingDisplay3/CNST-I-01-04-A?OpenDocument

Convened by the Committee on National Statistics (CNSTAT), Division of Behavioral and Social Sciences and Education within The National Academies.

October 16-17, 2003.

Chair: Eleanor Singer

Sessions:

I. Data Access and Confidentiality—the Changing Legal Landscape
II. Facilitating Data Access
III. Measuring the Risks and Costs of Disclosure: to the Data Enterprise, to Individuals
IV. The Impact of Multiple Imputation on Disclosure Risk and Informational Utility
V. Assessing the Benefits of Researcher Access to Longitudinal Microdata
VI. Assessing Research and Policy Needs and Confidentiality Concerns: The Economics of Data Access

Papers and Presentations: Available on website under Publications
http://www7.nationalacademies.org/cnstat/Data_Access_Panel.html

Workshop on Improving Access to and Confidentiality of Research Data
http://books.nap.edu/catalog/9958.html

Convened by the Committee on National Statistics (CNSTAT), Division of Behavioral and Social Sciences and Education within The National Academies in consultation with the Institute of Medicine.

October 1999.

Purpose: To identify ways of advancing the often conflicting goals of exploiting the research potential of microdata and preserving confidentiality, with an emphasis on longitudinal data that are linked to administrative records.

Chair: Norman Bradburn, National Opinion Research Center

Report: *Improving Access to and Confidentiality of Research Data: Report of a Workshop* (NRC, 2000)

Privacy and Confidentiality & Conflicts of Interest: Keeping Pace with Research Practices

Convened by Columbia University Center for Bioethics and sponsored by NIH with the Mailman School of Public Health and the Columbia School of Nursing

May 30, 2003.

Participants: More than 150 investigators, IRB members, research administrator, and others

Goal: To share latest developments and critical information that affects current practices in research regarding privacy and confidentiality and conflicts of interest.

Reports

Institute of Medicine (1994). *Health Data in the Information Age*. Committee on Regional Health Data Networks, Division of Health Care Services. Donaldson, M.S. and K.N. Lohr, eds. Washington DC: National Academy Press. http://books.nap.edu/books/0309049954/html/index.html.

Institute of Medicine (2001). *Preserving Public Trust: Accreditation and Human Research Participant Protection Programs*. Committee on Assessing the System for Protecting Human Research Participants, Board on Health Sciences Policy. Washington DC: National Academy Press. http://books.nap.edu/catalog/10085.html.

Institute of Medicine (2002). *Responsible Research: A Systems Approach to Protecting Research Participants*. Committee on Assessing the System for Protecting Human Research Participants, Board on Health Sciences Policy, Institute of Medicine. D. Federman, K. Hanna, and L. Lyman Rodriquez, eds. Washington DC: National Academies Press. http://www.nap.edu/catalog/10508.html; http://www.iom.edu/includes/dbfile.asp?id=4157

National Research Council (2000). *Improving Access to and Confidentiality of Research Data: Report of a Workshop.* Committee on National Statistics (CNSTAT). C. Mackie and N. Bradburn, Eds. Commission on Behavioral and Social Sciences and Education. Washington DC: National Academies Press**.** http://books.nap.edu/catalog/9958.html (accessed 24 March 2004).

National Research Council (2003). *Protecting Participants and Facilitating Social and Behavioral Sciences Research.* Panel on Institutional Review Boards, Surveys, and Social Science Research. C. F. Citro, D.R. Ilgen, and C.B. Marrett, eds. Committee on National Statistics and Board on Behavioral Cognitive, and Sensory Sciences. Washington DC: The National Academies Press. http://books.nap.edu/catalog/10638.html (accessed 24 March 2004).

National Research Council (2003). Committee on National Statistics (CNSTAT), Panel on Confidential Data Access for Research Purposes. *Papers and Presentations.* Workshop on Data Access and Confidentiality, Access to Research Data: Assessing Risks and Opportunities, National Academy of Sciences, Washington DC, 16-17 October 2003. http://www7.nationalacademies.org/cnstat/Data_Access_Panel.html

National Research Council and Social Science Research Council (1993)**.** *Private Lives and Public Policies: Confidentiality and Accessibility of Government Statistics*. Panel on Confidentiality and Data Access. G.T. Duncan, T.B. Jabine, and V.A. de Wolf, eds. Committee on National Statistics, Commission on Behavioral and Social Sciences and Education. Washington DC: National Academy Press. http://books.nap.edu/books/0309047439/html/index.html (accessed 24 March 2004).

U.S. Department of Health and Human Services (US DHHS) Centers for Disease Control and Prevention and Council of State and Territorial Epidemiologists (2003, draft). *CDC-CSTE Intergovernmental Data Release Guidelines Working Group (DRGWG) Report: CDC-ATSDR-CSTE Data Release Guidelines for Re-release State Data.* Draft report for soliciting input and feedback (drgwg report ver 6-2.doc).

http://www.cdc.gov/nchs/data/phdsc/drgwg%20report%20ver%20621.pdf (accessed March 30, 2004).

U.S. Office of Management and Budget (1994). *Report on Statistical Disclosure Limitation Methodology*. Subcommittee on Disclosure Limitation Methodology, Federal Committee on Statitistical Methodology. Statistical Policy Working Paper 22. 1994. Accessed at http://www.fcsm.gov/working-papers/spwp22.html (accessed 18 March 2004).

U.S. Office of Management and Budget (1999). *Checklist on Disclosure Potential of Proposed Data Releases*. Interagency Confidentiality and Data Access Group, An Interest Group of the Federal Committee on Statistical Methodology. Accessed at http://www.fcsm.gov/committees/cdac/checklist_799.doc (accessed 18 March 2004).

U.S. Office of Management and Budget (2001). *Confidentiality and Data Access Issues Among Federal Agencies*. Confidentiality and Data Access Committee and Federal Committee on Statistical Methodology. http://www.fcsm.gov/committees/cdac/brochur10.pdf (accessed 18 March 2004).

Appendix IV: Selected Bibliography[*]

Aboud, J.M., and S.D. Woodcock (2002). Disclosure limitation in longitudinal linked data. In *Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies*, P. Doyle, J.I. Lane, J.J.M. Theeuwes, and L.V. Zayatz, eds. Amsterdam, North Holland: Elsevier, pp. 215-278. http://books.nap.edu/books/0309071801/html/38.html#pagetop (accessed 11 March 2005).

Abrams, N., and M.D. Buckner, Eds. (1994). *Medical Ethics: A Clinical Textbook and Reference for the Health Care Professionals*. Cambridge MA: MIT Press.

Agency for Toxic Substances and Disease Registry (ATSDR) Web Site, June 12, 2003. http://www.cdc.gov/od/foia/foi.htm (accessed 18 August 2003).

Amendment No. 59. S1413. U.S. Senate, 2003. http://www.epic.org/privacy/profiling/tia/sa59.html (accessed 11 March 2005).

American Statistical Association (ASA), Committee on Privacy and Confidentiality (2003a). *American Statistical Association's Privacy, Confidentiality, and Data Security Website.* http://www.amstat.org/comm/cmtepc/index.cfm?fuseaction=content (accessed 11 March 2005).

American Statistical Association (ASA), Committee on Privacy and Confidentiality (2003b). *Welcome to the American Statistical Association's Privacy, Confidentiality, and Data Security Website.* http://www.amstat.org/comm/cmtepc/index.cfm (accessed 11 March 2005).

Annas, G.J. (2003). HIPAA regulations - A new era of medical-record privacy? *The New England Journal of Medicine* **348**(15):1486-1490.

Appelbaum, P.S. (2000). Protecting privacy while facilitating research. *Am J Psychiatry* **157**(11):1725-1726. http://ajp.psychiatryonline.org (accessed 11 July 2003).

Appelbaum, P.S. (2000). Threats to the confidentiality of medical records—no place to hide. *Journal of the American Medical Association* **283**(6):795-797. http://jama.ama-assn.org (accessed 11 July 2003).

Armstrong, M.P., G. Rushton, and D. Zimmerman (1999). Geographically masking health data to preserve confidentiality. *Statistics in Medicine* **18**(5):497-525. http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&list_uids=10209808&dopt=Abstract (accessed 11 March 2005)..

Bayer, R., and A.L. Fairchild (2000). Surveillance and privacy. *Public Health and Medicine* **290**:1898-1899.

Beck, L.R., B.M. Lobitz, *et al.* (2000). Remote sensing and human health: New sensors and new opportunities. *Emerging Infectious Diseases* **6**(3):217-227.

Bedard, Y., P. Gosselin, *et al.* (2003). Integrating components with knowledge discovery technology for environmental health decision support. *International Journal of*

[*] Note: Some links given here may require a subscription to an online service.

Medical Informatics **70**(1):79-94. http://www.sciencedirect.com/science/article/B6T7S-48BJX5D-2/2/e2091e7fb4e111f0c3829930fa75c29f (accessed 11 July 2003).

Blakemore, M. (2002). The potential and perils of remote access. In *Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies*, P. Doyle, J.I. Lane, J.J.M. Theeuwes, and L.V. Zayatz, eds. Amsterdam, North Holland: Elsevier, pp. 315-340.

Buckeridge, D.L., R. Mason, *et al.* (2002). Making health data maps: a case study of a community/university research collaboration. *Social Science & Medicine* 55(7): 1189-1206. http://www.sciencedirect.com/science/article/B6VBF-46MC8C1-9/2/7c8bbcc5b24e1d682fbb5931d1a1558b (accessed 11 March 2005).

Carretta, H.J., and S.S. Mick (2003). Geocoding public health data. *Am J Public Health* **93**(5):699-699. http://www.ajph.org/cgi/content/full/93/5/699 (accessed 11 July 2003).

Center for Bioethics, Columbia University (2003). *Privacy and Confidentiality and Conflicts of Interest: Keeping Pace with Research Practice,* Hammer Health Sciences Building, Columbia University, New York.

Centers for Disease Control Web Site, August 18, 2003. http://www.cdc.gov/ (accessed 19 August 2003).

Chadee, D.D. and U. Kitron (1999). Spatial and temporal patterns of imported malaria cases and local transmission in Trinidad. *American Journal of Tropical Medicine & Hygiene* **61**(4):513-517.

Clarke, K.C., J.P. Osleeb, *et al.* (1991). The use of remote-sensing and geographic information systems in UNICEF's Dracunculiasis (Guinea Worm) eradication effort. *Preventive Veterinary Medicine* **11**(3-4):229-235.

Clough, J.D., D.W. Rowan, and D.E. Nickelson (1999). Keeping our patients' secrets. *Cleveland Clinic Journal of Medicine* **66**(9):554-558.

Colwell, R.R. (1996). Global climate and infectious disease: The Cholera paradigm. *Science* **274**(5295):2025-31.

Committee on Basic Research in the Behavioral and Social Sciences (1988). The research support system. *The Behavioral and Social Sciences: Achievements and Opportunities*. Washington DC: National Academy Press, pp. 203-236. http://www.nap.edu/catalog/992.html (accessed 25 June 2003).

Computer Matching and Privacy Protection Act (CMPPA) of 1988 (1988). Public Law No. 100-503. 100th Congress. As Amended by Public Law No. 101-508. 101st Congress. http://www4.law.cornell.edu/uscode/5/552a.html (accessed 11 March 2005).

Computer Security Act of 1987 (1987). Public Law 100-255, 100th Congress. *Statutes at Large*. 101 Stat. 1724-1730. http://www.house.gov/science_democrats/archive/compsec1.htm (accessed 11 March 2005).

Confidential Information Protection and Statistical Efficiency Act, E-Government Act of 2002 Title V (2002). Public Law 107-347, 107th Congress. *United States Statutes at*

Large. 116 Stat. 2962. December 17, 2002. http://www.aiprp.gouv.qc.ca/publications/pdf/getdoc%5B1%5D.pdf (accessed 11 March 2005).

Coughlin, S.S., and T.L. Beauchamp, Eds. (1996). *Ethics and Epidemiology*. New York, Oxford University Press.

Cox, L.H. (1996). Protecting confidentiality in small population health and environmental statistics. *Statistics in Medicine* **15**(17-18):1895-1905. http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&list_uids=8888482&dopt=Abstract (accessed 11 March 2005).

Cox, L.H., McDonald, S.-K. and D. Nelson (1986). Confidentiality issues at the United States Bureau of the Census. *Journal of Official Statistics* **2**:135-160.

Croner, C. M. (2003). A healthy perspective on spatial data standards and interoperability, *Directions Magazine*. 2003.

Croner, C.M. (1996). Geographic Information Systems (GIS): New perspectives in understanding human health and environmental relationships. *Statistics in Medicine* **15**:1961-1977.

Croner, C.M. (2003). Public health GIS and the Internet. *Annual Review of Public Health* **24**:57-82. http://www/cdc.gov/nchs/data/gis/ GIS_AND_THE_INTERNET.pdf (accessed 11 March 2005).

Curry, M.R. (1997). The digital individual and the pivate realm. *Annals of the Association of American Geographers* **87**(4):681-699.

Dale, P.E., and C.D. Morris (1996). Culex annulirostris breeding sites in urban areas: Using remote sensing and digital image analysis to develop a rapid predictor of potential breeding areas. *Journal of the American Mosquito Control Association* **12**(2 Pt 1):316-20.

Day, J.F. (2001). Predicting St. Louis Encephalitis virus epidemics: Lessons from recent, and not so recent, outbreaks. *Annual Review of Entomology* **46**:111-138.

Detmer, D. (2003). Building the national health information infrastructure for personal health, health care services, public health, and research. *BMC Medical Informatics and Decision Making* **3**(1):1. http://www.biomedcentral.com/1472-6947/3/1 (accessed 11 July 2003).

de Wolf, V.A. (2003). Issues in accessing and sharing confidential survey and social science data. *Data Science Journal* **2**(17):66-74. http://www.codata.org/codata02/11datapolicy/deWolf/deWolf-paper.pdf (accessed 11 March 2005).

Digital Government Project Web Site. National Institute of Statistical Sciences, December 14, 2002. http://www.niss.org/dg/ (accessed 12 August 2003).

Dister, S.W., D. Fish, *et al.* (1997). Landscape characterization of peridomestic risk for Lyme disease using satellite imagery. *American Journal of Tropical Medicine & Hygiene* **57**(6):687-92.

Domingo-Ferrer, J., and V. Torra (2002). A quantitative comparison of disclosure control methods for microdata. In *Confidentiality, Disclosure and Data Access: Theory and*

Practical Applications for Statistical Agencies, P. Doyle, J.I. Lane, J.J.M. Theeuwes, and L.V. Zayatz, eds. Amsterdam, North Holland: Elsevier, pp. 111-134.

Doyle, P., J.I. Lane, J.J.M. Theeuwes, and L.V. Zayatz, Eds. (2002). *Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies*. Amsterdam, North Holland: Elesevier. http://www.elsevier.com/wps/find/bookdescription.cws_home/622129/description#description (accessed 11 March 2005).

Duncan, G.T. (2003). *Exploring the Tension between Privacy and the Social Benefits of Governmental Databases*. Security, Technology, and Privacy: Shaping a 21st Century Public Information Policy, Georgetown University Law Center, Washington DC.

Duncan, G.T., Jabine, T.B., and V. de Wolf (1993). *Private Lives and Public Policies: Confidentiality and Accessibility of Government Statistics*. Washington DC, National Academy Press.

Duncan, G.T., S.E. Feinberg, R. Krishnan, R. Padman, and S.F. Roehrig (2002). Disclosure limitation methods and information loss for tabular data. In *Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies*, P. Doyle, J.I. Lane, J.J.M. Theeuwes, and L.V. Zayatz, eds. Amsterdam, North Holland: Elsevier, pp. 135-166.

Dunne, T. (2002). Issues in the establishment and management of secure research sites. In *Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies*, P. Doyle, J.I. Lane, J.J.M. Theeuwes, and L.V. Zayatz, eds. Amsterdam, North Holland: Elsevier, pp. 297-314.

E-Government Act of 2002 (2002). HR 2458. Public Law 107-347, 107th Congress. *United States Statutes at Large*. 116 Stat. 2899. http://www.aiprp.gouv.qc.ca/publications/pdf/getdoc%5B1%5D.pdf (accessed 11 March 2005).

E-Government Act of 2002. U.S. Department of Education, May 6, 2003. http://www.ed.gov/offices/OCIO/legislation/egov.html (accessed 11 August 2003).

Electronic Privacy Information Center. 2003. *Open Government*. http://www.epic.org/open_gov/ (accessed 9 October 2003).

Etzioni, A. (1999). *The Limits of Privacy*. New York, Basic Books.

Fact Sheet: Strengthening Intelligence to Better Protect America. The White House, January 2003. http://www.whitehouse.gov/news/releases/2003/01/20030128-12.html (accessed 12 August 2003).

Federal Information Security Management Act of 2002, E-Government Act of 2002 Title III (2002). Public Law 107-347, 107th Congress. *United States Statutes at Large*. 116 Stat. 2946. December 17, 2002. http://www.aiprp.gouv.qc.ca/publications/pdf/getdoc%5B1%5D.pdf (accessed 11 March 2005).

Federal Policy for the Protection of Human Subjects (Basic DHHS Policy for Protection of Human Research Subjects, "The Common Rule") (1991a). Revised as of June 18, 1991. *Code of Federal Regulations* Title 45, Part 46 *Protection of Human Subjects*,

Subpart A. 56 FR 28003. http://www.hhs.gov/ohrp/references/frcomrul.pdf (accessed 11 March 2005).

Federal Policy for the Protection of Human Subjects (Basic DHHS Policy for Protection of Human Research Subjects, "The Common Rule") (1991b). Revised as of June 18, 1991. *Title 14—Aeronautics and Space, Chapter V—National Aeronautics and Space Administration, Part 1230—Protection of Human Subjects,* 14 CFR Part 1230, *Federal Register 56:117*, (18 June 1991): 28019.

Federal Policy for the Protection of Human Subjects (Basic DHHS Policy for Protection of Human Research Subjects, "The Common Rule") (2001). Revised as of November 13, 2001. *Code of Federal Regulations* Title 45, Part 46 *Protection of Human Subjects, Subpart A.* http://www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.htm#subparta (accessed 11 March 2005).

FedStats. *The Gateway to Statistics from over 100 U.S. Federal Agencies*. July 3, 2001. http://www.fedstats.gov/ (accessed 12 August 2003).

Felso, F., J. Theeuwes, and G.G. Wagner (2002). Disclosure limitation methods in use: Results of survey. In *Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies*, P. Doyle, J.I. Lane, J.J.M. Theeuwes, and L.V. Zayatz, eds. Amsterdam, North Holland: Elsevier, pp. 17-42.

Foley, R. (2002). Assessing the applicability of GIS in a health and social care setting: Planning services for informal carers in East Sussex, England. *Social Science & Medicine* **55**(1):79-96. http://www.sciencedirect.com/science/article/B6VBF-45X00VD-7/2/5cf9d9b437b53e4307fdac1e82c3af7a (accessed 11 March 2005).

Freedom of Information Act (1996b). 5 U.S.C. 552, As Amended by Public Law No. 104-231. 104th Congress. *United States Statutes at Large*. 110 Stat. 3048. http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm (accessed 11 March 2005).

Fuentes, M.V., J.B. Malone, *et al.* (2001). Validation of a mapping and prediction model for human Fasciolosis transmission in Andean very high altitude endemic areas using remote sensing data. *Acta Tropica* 79(1):87-95.

Gabrynowicz, J.I. (2003). Data, information, confidentiality and the legal landscape. Paper presented at the NASA Public Health Applications Program Confidentiality & Geospatial Data Workshop, 16 July 2003, Washington DC.

Giesing, S. (2002). Nonperturbative disclosure control methods for tabular data. In *Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies*, P. Doyle, J.I. Lane, J.J.M. Theeuwes, and L.V. Zayatz, eds. Amsterdam, North Holland: Elsevier, pp. 185-214.

Glass, G.E., J.E. Cheek, *et al.* (2000). Using remotely sensed data to identify areas at risk for Hantavirus Pulmonary Syndrome. *Emerging Infectious Diseases* **6**(3):238-247.

Hawala, S. (2000). On the variation of the percent of uniques in a microdata sample and the sample size. Upublished paper, June 2000, cited in *Zip Code Tabulation Area and Confidentiality* by the National Center for Health Statistics (NCHS), Centers for Disease Control and Prevention (2003).

Health Insurance Portability and Accountability Act of 1996 (HIPAA) (1996a). Public Law 104-191, 104th Congress. *United States Statutes at Large*. 110 Stat. 1936. http://aspe.hhs.gov/admnsimp/pl104191.htm (accessed 11 March 2005).

Hyman, S.E. (2000). The needs for database research and for privacy collide. *American Journal of Psychiatry* **157**(11):1723-1724.

Institute of Medicine (1994). *Health Data in the Information Age*. Committee on Regional Health Data Networks, Division of Health Care Services. M.S. Donaldson and K.N. Lohr, eds. Washington DC: National Academy Press. http://books.nap.edu/books/0309049954/html/index.html (accessed 11 March 2005).

Institute of Medicine (2002). *Responsible Research: A Systems Approach to Protecting Research Participants*. Committee on Assessing the System for Protecting Human Research Participants, Board on Health Sciences Policy, Institute of Medicine. D. Federman, K. Hanna, and L. Lyman Rodriquez, eds. Washington DC: National Academy Press. http://www.nap.edu/catalog/10508.html; http://www.iom.edu/includes/dbfile.asp?id=4157.

International Statistical Institute (1986). Declaration of professional ethics. *International Statistical Review* **54**:227-242.

Jabine, T.B. (1993a). Procedures for restricted data access. *Journal of Official Statistics* **9**:37-590.

Jabine, T.B. (1993b). Statistical disclosure limitation practices of United States statistical agencies. *Journal of Official Statistics* **9**:427-454.

Jacquez, G.M. and D.I. Greiling (2002). The geographic distribution of breast, lung and colorectal cancer in Long Island. *International Journal of Health Geographics* **2**:3. http://www.ij-healthgeographics.com/content/2/1/3 (accessed 13 March 2005).

Karr A.F. *et al.* (2002). Web-based systems that disseminate information from data but protect confidentiality. *Advances in Digital Government*. W.J. McIver, Jr. and A.K. Elmagarmid, eds. Amsterdam: Kluwer Press.

Kilbridge, P. (2003). The cost of HIPAA compliance. *The New England Journal of Medicine* **348**(15):1423-1424.

Kistemann, T., F. Dangendorf, and J. Schweikart (2002). New perspectives on the use of Geographic Information Systems (GIS) in the environmental health sciences. *International Journal of Hygiene and Environmental Health* **205**(3):161-181. http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&list_uids=12040915&dopt=Abstract (accessed 11 March 2005).

Kitron, U., and J.J. Kazmierczak (1997). Spatial analysis of the distribution of Lyme disease in Wisconsin. *American Journal of Epidemiology* **145**(6):558-566.

Krieger, N., J.T. Chen, P.D. Waterman, M.-J. Soobader, S.V. Subramanian, and R. Carson (2002). Geocoding and monitoring of US socioeconomic inequalities in mortality and cancer incidence: Does the choice of area-based measure and geographic level matter?: The Public Health Disparities Geocoding Project. *Am. J. Epidemiol.*

156(5):471-482. http://aje.oupjournals.org/cgi/content/full/156/5/471 (accessed 11 July 2003).

Krieger, N., Waterman, P.D., Chen, J.T., Soobader, M., and S.V. Subramanian (2003). Monitoring socioeconomic inequalities in sexually transmitted infections, tuberculosis, and violence: Geocoding and choice of area-based socioeconomic measures - The Public Health Disparities Geocoding Project (US). *Public Health Reports* **118**:240-260. http://phr.oupjournals.org/cgi/reprint/118/3/240.pdf (accessed 11 July 2003).

Krieger, N., J.T. Chen, P.D. Waterman, M.-J. Soobader, S.V. Subramanian, and R. Carson (2002). ZIP code caveat: Bias due to spatiotemporal mismatches between ZIP codes and US Census-defined geographic areas - The Public Health Disparities Geocoding Project. *Am J Public Health* **92**(7):1100-1102. http://www.ajph.org/cgi/content/full/92/7/1100 (accessed 11 July 2003).

Kusumayati, A., and R. Gross (1998). Ecological and geographic characteristics predict nutritional status of communities: Rapid assessment for poor villages. *Health Policy and Planning* **13**(4):408-16.

Lambert, D. (1993). Measures of disclosure risk and harm. *Journal of Official Statistics* **9**:313-331.

Liverman, D., E.F. Moran, R.R. Rindfuss, and P.C. Stern, Eds. (1998). *People and Pixels: Linking Remote Sensing and Social Science*. Washington DC: National Academy Press. http://www.nap.edu/books/0309064082/html/R7.html (accessed 11 July 2003).

Madsen, P. (2003). The ethics of confidentiality. Paper presented at the NASA Public Health Applications Program Confidentiality & Geospatial Data Workshop, 16 July 2003, Washington DC.

Malone, J.B., D.P. Fehler, *et al.* (1992). Use of LANDSAT MSS imagery and soil type in a geographic information system to assess site-specific risk of Fascioliasis on Red River Basin farms in Louisiana. *Annals of the New York Academy of Sciences* **653**:389-97.

Manager's Guide to Data Privacy. The Open Group, April 1, 2003. http://www.opengroup.org/publications/catalog/g033.htm (accessed 11 August 2003).

Marrett, C. (2002). *Letter from the Chair of the Panel on IRBs, Surveys, and Social Science Research, Committee on National Statistics, to Dr. Daniel Federman, Chair, Committee on Assessing the System for Protecting Human Research Participants, Institute of Medicine, July 1, 2002*. http://www7.nationalacademies.org/cnstat/IRB_Panel.html (accessed 11 March 2005).

Martin, D., and G. Higgs (1997). Population georeferencing in England and Wales: Basic spatial units reconsidered. *Environment and Planning* **29**(2):333-347.

Mayer, T. (2002). *Privacy and Confidentiality Research and the U.S. Census Bureau: Recommendations Based on a Review of the Literature*. Research Report Series, U.S. Bureau of the Census. 1-50, February 7, 2002.

Maynard, N.G. (2002). Remote sensing for public health surveillance and response. *Earth Observation Magazine.* http://www.eomonline.com/Common/currentissues/Aug02/maynard.htm (accessed 11 July 2003).

Meador, M., and A.J. Ruggles (2000). Steps involved in randomizing the coordinates of address-matched locations. *Public Health GIS News and Information* **35**:11-12. http://www.cdc.gov/nchs/gis.htm (accessed 11 July 2003).

Moncayo, A.C., J.D. Edman, *et al.* (2000). Application of geographic information technology in determining risk of Eastern Equine Encephalomyelitis virus transmission. *Journal of the American Mosquito Control Association* **16**(1):28-35.

Moreno, J., Caplan, A.L., Wolpe, P.R., and the Members of the Project on Informed Consent, Human Research Ethics Group (1998). Updating protections for human subjects involved in research. *Journal of the American Medical Association* **280**(22):1951-1958.

NASA Ames Research Center (2004). Life Scientists at Ames: Musculoskeletal Research—Robert T. Whalen. Ames Research Center website. NASA Johnson Space Center. (1996). *JSC Institutional Review Board Guidelines for Investigators Proposing Human Research for Space Flight and Related Investigations*. http://jsc-web-pub.jsc.nasa.gov/psrp/docs/JSC20483.pdf (accessed 11 March 2005).

NASA Johnson Space Center (2002). *NASA/JSC Human Research Informed Consent.*

NASA Office of Inspector General (2001). *Assessment of the Institutional Review Board for Human Subject Protection at the Johnson Space Center, G-01-002*. Letter to NASA Administrator from David M. Cushing, NASA Inspector General, on October 9, 2001. http://www.hq.nasa.gov/office/oig/hq/inspections/g-01-002.pdf (accessed 11 March 2005).

NASA Online Directives Information System Library (2003). http://nodis.gsfc.nasa.gov/library/main_lib.html (accessed 12 August 2003).

NASA Policy Directive (NPD) (2002). *Protection of Human Subjects* (NPD 7100.8D). http://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PD_7100_008D_&page_name=main (accessed 11 March 2005).

NASA Policy Directive (NPD) (2003). *Privacy Act—Internal NASA Direction in Furtherance of NASA Regulation (NPD 1382.17F).* http://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PD_1382_017F_&page_name=main (accessed 11 March 2005).

NASA Procedural Requirements (NPR) (1998). *Guidelines for Documentation, Approval, and Dissemination of NASA Scientific and Technical Information (STI).* (NPR 2200.2A, effective September 3, 1998). http://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PR_2200_002A_&page_name=main (accessed 11 March 2005).

NASA Procedural Requirements (NPR) (1999). *Security of Information Technology.* (NPR 2810.1, effective August 16, 1999). http://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PR_2810_0001_&page_name=main (accessed 11 March 2005).

NASA Procedural Requirements (NPR) (2003). *Protection of Human Research Subjects* (NPG 7100.1, effective March 28, 2003). http://nodis3.gsfc.nasa.gov/library/displayDir.cfm?Internal_ID=N_PG_7100_0001_&page_name=main (accessed 11 March 2005).

NASA Public Health Applications Program (PHAP) (2003). *NASA Public Health Applications Program Confidentiality & Geospatial Data Workshop*. Organized by the Socioeconomic Data and Applications Center (SEDAC). Hosted at the National Academies of Sciences Keck Center, Washington DC, 16 July 2003.

National Cancer Institute (2002). *Geographical Information System for Health.* http://www.healthgis-li.com/researchers/researchers.htm (accessed 11 July 2003).

National Center for Health Statistics (NCHS), Centers for Disease Control and Prevention. (2003). *Zip Code Tabulation Area and Confidentiality*. Joint ECE/Eurostat Work Session on Statistical Data Confidentiality, Conference of European Statisticians, Luxembourg, 7-9 April 2003, sponsored by United Nations Statistical Commission and Economic Commission for Europe and European Commission, Statistical Office of the European Communities (EUROSTAT). http://www.unece.org/stats/documents/2003/04/confidentiality/wp.34.e.pdf (accessed 11 March 2005).

National Center for Health Statistics (NCHS) Web Site, August 15, 2003. http://www.cdc.gov/nchs/ (accessed 11 March 2005).

National Institute of Communicable Diseases (NICD) Web Site. http://www.nicd.org/AboutNICD.asp (accessed 11 March 2005).

National Institutes of Health (NIH) (2002). Office of Extramural Research. *Certificates of Confidentiality*. http://grants1.nih.gov/grants/policy/coc/ (accessed 11 March 2005).

National Institutes of Health (NIH) (2003). *NIH Statement on Sharing Research Data, National Institutes of Health.* http://grants.nih.gov/grants/policy.datasharing/ (Accessed on 11 July 2003).

National Research Council (2000). *Improving Access to and Confidentiality of Research Data: Report of a Workshop.* Committee on National Statistics, Commission on Behavioral and Social Sciences and Education. C. Mackie and N. Bradburn, eds. Washington DC: National Academy Press. http://books.nap.edu/books/0309071801/html/index.html.

National Research Council (2003). *Protecting Participants and Facilitating Social and Behavioral Sciences Research.* Panel on Institutional Review Boards, Surveys, and Social Science Research. C. F. Citro, D.R. Ilgen, and C.B. Marrett, eds. Committee on National Statistics and Board on Behavioral, Cognitive, and Sensory Sciences. Washington DC: National Academy Press. http://books.nap.edu/catalog/10638.html (accessed 24 March 2004).

National Research Council (2003). Committee on National Statistics (CNSTAT), Panel on Confidential Data Access for Research Purposes. *Papers and Presentations.* Workshop on Data Access and Confidentiality, Access to Research Data: Assessing Risks and Opportunities, National Academy of Sciences, Washington DC, 16-17 October 2003. http://www7.nationalacademies.org/cnstat/Data_Access_Panel.html

National Science Foundation (NSF) (1999). Directorate for Computer and Information Science and Engineering, Division of Experimental and Integrative Activities. *Digital Government Program Announcement NSF 99-103.*

National Science Foundation (NSF) (2003). *NSF Confidentiality Workshop*. 2003. http://www.urban.org/nsfpresentations/index.html (accessed 11 March 2005).

O'Dwyer, L.A., and D.L. Burton (1998). Potential meets reality: GIS and public health research in Australia. *Australian and New Zealand Journal of Public Health* **22**(7):819-823. http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&list_uids=9889450&dopt=Abstract (accessed 11 March 2005).

Olvingson, C., J. Hallberg, T. Timpka, and K. Lindqvist (2003). Ethical issues in public health informatics: Implications for system design when sharing geographic information. *Journal of Biomedical Informatics* **35**(3):178-185. http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&list_uids=12669981&dopt=Abstract (accessed 11 March 2005).

Phillips, R.L., E.L. Kinman, P.G. Schnitzer, E.J. Lindbloom, and B. Ewigman (2000). Using Geographic Information Systems to understand health care access. *Archives of Family Medicine* **9**(10):971-978. http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&list_uids=11115195&dopt=Abstract (accessed 11 March 2005).

President's Commission on Federal Statistics (1971). *Federal Statistics. Vol. I.* Washington DC: U.S. Government Printing Office.

Privacy Act of 1974 (1974). 5 U.S.C. Sec. 552a, as amended, Washington DC: U.S. Department of Justice. http://www.usdoj.gov/foia/privstat.htm (accessed 11 March 2005).

Privacy Act – NASA Regulations (1999). Revised as of January 1, 1999. *Code of Federal Regulations* Title 14, Volume 5, Part 1212. Washington DC: U.S. Government Printing Office. http://www.access.gpo.gov/nara/cfr/waisidx_99/14cfr1212_99.html (accessed 11 March 2005).

Private Property Protection Act of 1995 (1995). HR 925 EH. House of Representatives, March 3, 1995. http://classweb.gmu.edu/jkozlows/hr925.htm (accessed 12 August 2003).

Randolph, S.E. (2001). The shifting landscape of tick-borne zoonoses: Tick-borne encephalitis and Lyme borreliosis in Europe. *Philosophical Transactions of the Royal Society of London Series B-Biological Sciences* **356**(1411):1045-1056.

Richards, T.B., C.M. Croner, G. Rushton, C.K. Brown, and L. Fowler (1999). Geographic Information Systems and public health: Mapping the future. *Public Health Reports* **114**:359-373. http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&list_uids=10501137&dopt=Abstract (accessed 11 July 2003).

Rindfuss, R.R. (2002). Conflicting demands: Confidentiality promises and data availability. *IHDP Update: Newsletter of the International Human Dimensions Programme on Global Environmental Change* (Feb. 2002), pp. 1-4, 8. http://www.ihdp.uni-

bonn.de/html/publications/update/update02_02/Update02_02_ art1.html (accessed 11 March 2005).

Rindfuss, R.R., and P.C. Stern (1998). Linking remote sensing and social science: The need and the challenges. *People and Pixels: Linking Remote Sensing and Social Science*. D. Liverman, Moran, E.F., Rindfuss, R.R., and P.C. Stern, eds. Washington DC, National Academy Press**.** pp. 1-27.

Rose, J.B., P.R. Epstein, *et al.* (2001). Climate variability and change in the United States: Potential impacts on water- and foodborne diseases caused by microbiologic agents. *Environmental Health Perspectives* **109**:211-221.

Rothstein, M.A. (1998). Genetic privacy and confidentiality: Why they are so hard to protect. *Journal of Law, Medicine & Ethics* **26**:198-204.

Rushton, G., and P. Lolonis (1996). Exploratory spatial analysis of birth defect rates in an urban population. *Statistics in Medicine* **15**(7-9):717-726.

Seastrom, M.M., C. Wright, and J. Melnicki (2003). The role of licensing and enforcement mechanisms in promoting access and protecting confidentiality. Workshop on Data Access and Confidentiality, Access to Research Data: Assessing Risks and Opportunities, October 16-17, 2003, National Academy of Sciences, Washington DC. http://www7.nationalacademies.org/cnstat/Data_Access_Panel.html.

Seastrom, M.M. (2002). Licensing. In *Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies*, P. Doyle, J. Lane, J.J.M. Theeuwes, and L. Zayatz, eds. Amsterdam, North Holland: Elsevier, pp. 279-296.

Seltzer, W., and M. Anderson (2002). NCES and the Patriot Act: An early appraisal of facts and issues. Paper presented at the Joint Statistical Meetings, New York, August 10-15, 2002. http://www.uwm.edu/~margo/govstat/jsm.pdf (accessed 13 March 2005).

Simons, B., and E. Spafford (2003). Letter to Senators John Warner and Carl Levin, Association for Computing Machinery, U.S. ACM Public Policy Committee, January 23, 2003. http://www.acm.org/usacm/Letters/tia_final.html (accessed 13 March 2005).

Steel, P., and J. Sperling (2001). *The Impact of Multiple Geographies and Geographic Detail on Disclosure Risk: Interactions between Census Tract and ZIP Code Tabulation Geography*. U.S. Census Bureau, unpublished monograph. www.census.gov/srd/sdc/steel.sperling.2001.pdf (accessed 11 March 2005).

Sweeney, L. (1997). Weaving technology and policy together to maintain confidentiality. *J Law Med Ethics* **25**:98-110.

Sweeney, L. (1998). Privacy and confidentiality, in particular, computational disclosure control (web page). http://lab.privacy.cs.cmu.edu/people/sweeney/confidentiality.html (accessed 13 March 2005).

Tarkan, L. (2003). A privacy law's unintended results. *The New York Times*. http://www.nytimes.com/2003/06/03/health/03PRIV.html?ex=1055645239&ei=1&en=17ee487ef38a6189 (accessed 13 March 2004).

Taylor, P. (2003). Privacy: A civilized luxury. *Government Technology* **46**.

Terrorism Information Awareness (Tia) System. DARPA Information Awareness Office, March 11, 2003. http://www.darpa.mil/iao/TIASystems.htm (accessed 12 August 2003).

Theseira, M. (2002). Using Internet GIS technology for sharing health and health related data for the West Midlands Region. *Health & Place* **8**:37-46. http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&list_uids=11852262&dopt=Abstract (accessed 11 July 2003).

Thompson, A.J., and D.L. Schmoldt (2001). Ethics in computer software design and development. *Computers and Electronics in Agriculture* **30**(1-3):85-102.

Thomson, M.C., and S.J. Connor (2000). Environmental information systems for the control of arthropod vectors of disease. *Medical & Veterinary Entomology* **14**(3):227-244.

Thomson, M.C., S.J. Connor, *et al.* (1999). Predicting malaria infection in Gambian children from satellite data and bed net use surveys: The importance of spatial correlation in the interpretation of results. *American Journal of Tropical Medicine & Hygiene* **61**(1):2-8.

Tim, U.S. (1995). The application of GIS in environmental health sciences: Opportunities and limitations. *Environ Res* **71**(2):75-88.

Total "Terrorism" Information Awareness (Tia). Electronic Privacy Information Center, May 30, 2003. http://www.epic.org/privacy/profiling/tia/ (accessed 12 August 2003).

USA PATRIOT ACT: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (2001). H.R. 3162. Public Law 107-56, 107th Congress. http://www.epic.org/privacy/terrorism/hr3162.pdf (accessed 11 March 2005).

U.S. Census Bureau (US Census), The Center for Economic Studies (CES) (2003). *Carnegie Mellon Research Data Center*. April 10, 2003. http://www.ces.census.gov/ces.php/home (accessed 11 March 2005).

U.S. Congress. House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform (2003). *Geographic Information Systems: Challenges to Effective Data Sharing.* Testimony by Linda D. Koontz, Director of Information Management Issues, U.S. General Accounting Office. Washington DC, June 10, 2003. GAO-03-874T. http://www.gao.gov/new.items/d03874t.pdf (accessed 11 March 2005).

U.S. Congress, Office of Technology Assessment (OTA) (1986). *Federal Government Information Technology: Electronic Record Systems and Individual Privacy. OTA-CIT-296*. Washington DC: U.S. Government Printing Office, June 1986. http://www.wws.princeton.edu/cgi-bin/byteserv.prl/~ota/disk2/1986/8606/_8606.PDF (accessed 11 March 2005).

U.S. Department of Commerce (DOC), National Bureau of Standards (NBS) (1975). *Computer Security Guidelines for Implementing the Privacy Act of 1974*. Federal Information Processing Standards Publication, FIPS PUB 41. Washington DC: Government Printing Office, May 30, 1975. http://www.itl.nist.gov/fipspubs/withdraw.htm (accessed 11 March 2005).

U.S. Department of Energy (US DOE), Office of Health and Environmental Research. (1996). NASA's new human subjects policy. *Protecting Human Subjects*, Fall 1996. http://www.er.doe.gov/production/ober/humsubj/fall96/fall9605.html (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS) Centers for Disease Control and Prevention (CDC) and Agency for Toxic Substances and Disease Registry (ATSDR) (2003). *CDC/ATSDR Procedures for Protection of Human Research Participants: 2003.* http://www.cdc.gov/od/ads/procphrp.pdf (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS) Centers for Disease Control and Prevention (CDC) and Council of State and Territorial Epidemiologists (CSTE) (2003 Draft). *CDC-CSTE Intergovernmental Data Release Guidelines Working Group (DRGWG) Report: CDC-ATSDR-CSTE Data Release Guidelines for Re-release State Data.* Draft report (drgwg report ver 6-2.doc).

U.S. Department of Health and Human Services (US DHHS) Centers for Disease Control and Prevention (CDC), Office for Science Policy and Technology Transfer (OSPTT) (2004). *Human Subjects Research.* http://www.cdc.gov/od/ads/hsr2.htm (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS), National Institutes of Health (NIH) (1995). Revised 2 March 1995. *Guidelines for the Conduct of Research Involving Human Subjects at the National Institutes of Health*. http://nihtraining.com/ohsrsite/guidelines/graybook.html (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS), National Institutes of Health (NIH) (2003a). *Certificates of Confidentiality Kiosk*. http://grants.nih.gov/grants/policy/coc/index.htm (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS), National Institutes of Health (NIH) (2003b). *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule*. http://privacyruleandresearch.nih.gov/pr_02.asp (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS), Office of Civil Rights (OCR) (2002). *Standards for Privacy of Individually Identifiable Health Information (The Privacy Rule), Final Modifications. Federal Register* **67** (August 14, 2002). *Code of Federal Regulations*, Title 45, Parts 160 and 164. http://www.hhs.gov/ocr/hipaa/finalreg.html (accessed 11 March 2005). http://privacyruleandresearch.nih.gov/ (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS), Office for Civil Rights (OCR) (2003). *Website on Medical Privacy- National Standards to Protect the Privacy of Personal Health Information*. http://www.hhs.gov/ocr/hipaa (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS). Office for Human Research Protections (OHRP) (2000a). *Human Subject Regulations Decision Charts*.

http://www.hhs.gov/ohrp/humansubjects/guidance/decisioncharts.htm (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS). Office for Human Research Protections (OHRP) (2000b). *Informed Consent Checklist.* http://www.hhs.gov/ohrp/humansubjects/assurance/consentckls.htm (accessed 11 March 2005)

U.S. Department of Health and Human Services (US DHHS). Office for Human Research Protections (OHRP) (2002). *Human Research Protections Database*. U.S. Department of Health and Human Services (US DHHS).

U.S. Department of Health and Human Services (US DHHS). Office for Human Research Protections (OHRP) (2003a). *Assurances and IRB Registration.* http://www.hhs.gov/ohrp/assurances/assurance_index.htm (accessed 11 March 2005). http://www.hhs.gov/ohrp/assurances/ (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS). Office for Human Research Protections (OHRP) (2003b). *Federalwide Assurance (FWA).* http://www.hhs.gov/ohrp/humansubjects/assurance/filasurt.htm (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS). Office for Human Research Protections (OHRP) (2003c). *Institutional Review Board (IRB) Registration.* http://www.hhs.gov/ohrp/assurances/ (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS). Office for Human Research Protections (OHRP) (2003d). *Policy Guidance.* http://hhs.gov/ohrp/policy/ (accessed 11 March 2005).

U.S. Department of Health and Human Services (US DHHS). Office for Human Research Protections (OHRP) (2004). *General OHRP Information*. http://hhs.gov/ohrp/ (accessed 11 March 2005).

U.S. Department of Justice (US DOJ). Office of Information and Privacy (2002, last updated*). FOIA Update (1979-2000).* http://www.usdoj.gov/oip/foi-upd.htm (accessed 11 March 2005).

U.S. General Accounting Office (US GAO), Health Services Quality and Public Health Issues (1999). *Medical Records Privacy: Access Needed for Health Research, But Oversight of Privacy Protections is Limited.* Report to Congress, 24 February 1999, GAO/HEHS-99-55. http://www.epic.org/privacy/medical/gao-medical-privacy-399.pdf (accessed 11 March 2005).

U.S. General Accounting Office (US GAO) (2001). *Record Linkage and Privacy: Issues in Creating New Federal Research and Statistical Information*. GAO-01-126SP. Washington DC, April 2001. http://www.gao.gov/new.items/d01126sp.pdf (accessed 11 March 2005).

U.S. Office of Management and Budget (US OMB) (1989). *Privacy Act of 1974; Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988. Federal Register* **54**:116 (1989): 25818-25829. http://www.dod.mil/privacy/1975OMB_PAGuide/jun1989.pdf (accessed 11 March 2005).

U.S. Office of Management and Budget (US OMB) (1990). *Circular No. A-16 Revised: Coordination of Surveying, Mapping, and Related Spatial Data Activities.* http://clinton4.nara.gov/textonly/OMB/circulars/a016/a016.html (accessed 11 March 2005)

U.S. Office of Management and Budget (US OMB) (2000a). Revision of Circular No. A-130, Transmittal No. 4: Management of Federal Information Resources. *Federal Register* **65**:239, 12 December 2000. http://www.ogc.doc.gov/ogc/contracts/cld/ecomm/65fr77677.html (accessed 11 March 2005).

U.S. Office of Management and Budget (US OMB) (2000b). *Memorandum for Heads of Executive Departments and Agencies: Guidance on Inter-Agency Sharing of Personal Data-Protecting Personal Privacy* (M-01-05), 20 December 2000. http://www.whitehouse.gov/omb/memoranda/m01-05.html (accessed 11 March 2005).

U.S. Office of Management and Budget (US OMB) (2002). *Circular No. A-16 Revised: Coordination of Geographic Information and Related Spatial Data Activities.* http://www.whitehouse.gov/omb/circulars/a016/text/a016_rev.html (accessed 11 March 2005).

U.S. Office of Management and Budget (US OMB) (2003). *Memorandum for Heads of Executive Departments and Agencies: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (M-03-22), 26 September 2003. http://www.whitehouse.gov/omb/memoranda/m03-22.html (accessed 11 March 2005).

U.S. Office of Management and Budget (US OMB). Federal Committee on Statistical Methodology (FCSM) (1994). *Report on Statistic Disclosure Limitation Methodology: Statistical Policy Working Paper 22*. http://www.fcsm.gov/working-papers/spwp22.html (accessed 11 March 2005).

U.S. Office of Management and Budget (US OMB). Federal Committee on Statistical Methodology (FCSM), Confidentiality and Data Access Committee (CDAC) (1999). *Checklist on Disclosure Potential of Proposed Data Releases.* http://www.fcsm.gov/committees/cdac/cdac.html (accessed 11 March 2005).

U.S. Office of Management and Budget (US OMB). Federal Committee on Statistical Methodology (FCSM), Confidentiality and Data Access Committee (CDAC) (2002). *Restricted Access Procedures: Confidentiality and Data Access Committee.* www.fcsm.gov/committees/cdac/cdacra9.pdf (accessed 11 March 2005).

U.S. Office of Management and Budget (US OMB). Federal Committee on Statistical Methodology (FCSM), Confidentiality and Data Access Committee (CDAC) (2004). *About CDAC.* http://www.fcsm.gov/committees/cdac/about.html (accessed 11 March 2005).

U.S. President, W.J. Clinton. Memorandum for the Vice President, the Heads of Executive Departments, and Agencies (1994). *Review of Federal policy for the Protection of Human Subjects*, February 17, 1994. http://www.hhs.gov/ohrp/humansubjects/guidance/hsdc94feb.htm (accessed 11 March 2005).

U.S. President's Advisory Committee on Human Radiation Experiments (ACHRE) (1995). *Final Report of the Advisory Committee on Human Radiation Experiments.* Washington DC: Government Printing Office (stock number 061-000-00-848-9). http://tis.eh.doe.gov/ohre/roadmap/achre/chap18.html (accessed 11 March 2005).

Vicente, G.A., and N. Maynard (2002). Integrated system for health applications of Earth science remote sensing data. *IAPRS* **34**(2):481-484. http://www.isprs.org/commission2/proceedings/paper/085_115.pdf (accessed 11 March 2005).

Ward, M.H., J.R. Nuckols, *et al.* (2000). Identifying populations potentially exposed to agricultural pesticides using remote sensing and geographic information system. *Environmental Health Perspectives* **108**(1):5-12.

Warren, S.D., and L.D. Brandeis (1890). The right to privacy. *Harvard Law Review* **IV**(5).

Xiang, H., J.R. Nuckols, *et al.* (2000). A geographic information assessment of birth weight and crop production patterns around mother's residence. *Environmental Research* **82**(2):160-7.

Yarborough, M., and R.R. Sharp (2002). Restoring and preserving trust in biomedical research. *Academic Medicine* **77**(1):8-14.

Zayatz, L.Y., P. Steel, and S. Rowland (2000). *Disclosure Limitation for Census 2000*. Proceedings of the Section on Government Statistics, Indianapolis, American Statistical Association.

Zenilman, J.M., G. Glass, T. Shields, P.R. Jenkins, J.C. Gaydos, and K.T. McKee, Jr. (2002). Geographic epidemiology of gonorrhoea and chlamydia on a large military installation: Application of a GIS system. *Sex. Transm. Inf.* **78**(1):40-44.