



TOURO UNIVERSITY
JACOB D. FUCHSBERG LAW CENTER
Where Knowledge and Values Meet

**Digital Commons @ Touro Law
Center**

Scholarly Works

Faculty Scholarship

2005

GIS in an Age of Homeland Security: Accessing Public Information to Ensure a Sustainable Environment

Patricia E. Salkin

Touro Law Center, psalkin@tourolaw.edu

Follow this and additional works at: <https://digitalcommons.tourolaw.edu/scholarlyworks>



Part of the [Environmental Law Commons](#), and the [State and Local Government Law Commons](#)

Recommended Citation

30 Wm. & Mary Envtl. L. Rev. 55 (2005).

This Article is brought to you for free and open access by the Faculty Scholarship at Digital Commons @ Touro Law Center. It has been accepted for inclusion in Scholarly Works by an authorized administrator of Digital Commons @ Touro Law Center. For more information, please contact lross@tourolaw.edu.

GIS IN AN AGE OF HOMELAND SECURITY: ACCESSING PUBLIC INFORMATION TO ENSURE A SUSTAINABLE ENVIRONMENT

PATRICIA E. SALKIN*

INTRODUCTION

Critical to the goal of achieving sustainable development is governments' ability to maintain public information, including maps, charts, statistics, and narrative text, about a wide variety of environmental factors, indicators, resources, and threats in easily understandable formats that are readily accessible to the public. While federal and state freedom of information laws help to ensure a relatively high rate of public access to traditional information, such as environmental impact statements, studies and reports, significant environmental events and resources, and census data, the growing use and reliance on geographic information systems ("GIS") has the potential to move the public discourse to a more sophisticated plane. GIS continues to be used as an effective planning tool, enabling users to access information relating to, among other things, existing conditions, environmental assessments, impact statements, transportation studies, and community studies.¹

GIS is a type of computerized mapping, yet it is not limited solely to map form because information about a location can be represented through charts, graphs or tables in ways that are

* Patricia E. Salkin is Associate Dean and Director of the Government Law Center of Albany Law School. Dean Salkin is grateful for the research assistance of Albany Law School students Michael Donohue, Jasper Mills, Allyson Phillips, and Alejandra Rosario. A part of the introduction to this article explaining GIS is excerpted from Patricia E. Salkin & Michael Donohue, *Geographic Information Systems for Land Use Lawyers* 101, 2004 N.Y. Zoning L. & Prac. Rep. 1-2 (Sept.-Oct. 2004).

¹ Javier Aguilar & Joanne Haracz, *Environmental Justice: Visualization and Analyses with GIS to Facilitate Informed Decisions*, <http://gis.esri.com/library/userconf/proc01/professional/papers/pap523/p523.htm> (last visited Nov. 15, 2005).

unavailable to traditional paper maps.² A GIS system is designed to “determine the capture, management, manipulation, analysis, modeling, and display of spatially-referenced data for solving complex planning and management problems.”³ Its purpose is to store and analyze objects and “phenomenon [sic] where geographic location is an important characteristic or critical to the analysis.”⁴ GIS has also been defined as “a spatial abstraction of the real world, including infrastructure, cultural, social, physical, economic, and other spatially related information, which abstraction is used to solve problems associated with the data whose common attributes are related to space and geography.”⁵ The New York State Geographical Information Systems (“NYS GIS”) Clearinghouse explains that “[t]he value of GIS and spatial data can be seen most dramatically in applications . . . that promote economic development, public health and safety, and environmental quality.”⁶

Used exclusively in federal military projects for approximately twenty-five years,⁷ today other branches of government as well as the private sector are able to use GIS in a variety of helpful ways. For example, GIS has been used to plot the best hurricane evacuation route,⁸ to plot the shortest route from a police or fire

² See generally ANDY MITCHELL, ZEROING IN: GEOGRAPHIC SYSTEMS AT WORK IN THE COMMUNITY xi-xxi (Environmental Systems Research Institute, Inc. 1997).

³ Bd. of Assessment App. v. AM/FM Int'l, 940 P.2d 338, 340 (1997); see also Jennifer L. Phillips, Comment, *Information Liability: The Possible Chilling Effect of Tort Claims Against Producers of Geographic Information Systems Data*, 26 FLA. ST. U. L. REV. 743, 745 (1999) (summarizing various descriptions and definitions of GIS which are used in the field).

⁴ Jeremy Speich, Comment, *The Legal Implications of Geographical Information Systems (GIS)*, 11 ALB. L.J. SCI. & TECH. 359, 361 (2001) (quoting STAN ARNOFF, GEOGRAPHIC INFORMATION SYSTEMS: A MANAGEMENT PERSPECTIVE 41 (1993)).

⁵ AM/FM Int'l, 940 P.2d at 340.

⁶ Executive Briefing Paper: Why Should You Consider Geographic Information Systems?, http://64.233.161.104/search?q=cache:_84OFm8oNbAJ:nysgis.state.ny.us/briefing.htm&hl=en&lr=&strip=0 (last visited Nov. 15, 2005).

⁷ Phillips, *supra* note 3, at 745 (citing ARNOFF, *supra* note 4, at 19, tbl.2).

⁸ Scott D. Makar & Micahel R. Makar Jr., *Geographic Information Systems: Legal and Policy Implications*, 69 FLA. BAR J. 44, n.1 (1995).

station to an accident scene or other emergency location,⁹ and to overlay specific crimes on a map in an attempt to glean patterns.¹⁰

GIS data collection is aided through the use of the Global Positioning System ("GPS"). The GPS was "[d]eveloped by the United States Department of Defense (DOD), . . . [and] utilizes a constellation of twenty-four satellites which orbit approximately 11,000 miles above the Earth."¹¹ The system is designed so that at any point in time there will be at least four satellites "in view" of a GPS receiver located anywhere on the globe."¹² The receiver measures its distance from the satellites to calculate its position on Earth.¹³ In 1995, GPS technology was made available for use by the general public.¹⁴

Currently, forty-two states along with the District of Columbia and Puerto Rico have laws relating to GIS systems. The majority of the laws require the establishment or maintenance of

⁹ MITCHELL, *supra* note 2, at 4.

¹⁰ Makar, *supra* note 8, at 44.

[A] database could contain spatial information on the Eisenhower Interstate System. Each interstate could have tabular information associated with it, including volume, average width and bridge tonnage. The spatial information is arranged in layers, or overlays, and each added layer, for example, flood plains, is laid out across the other. The tabular information is then linked with the spatial information, allowing each to be accessed by the other at a coordinate. This would enable an operator to map the safest and most efficient shipping route for sixty-ton trucks during the rainy season in Iowa, while also identifying potential trouble spots.

Speich, *supra* note 4, at 362 (citations omitted).

¹¹ James R. Walter, Note, *A Brand New Harvest: Issues Regarding Precision Agriculture Data Ownership and Control*, 2 DRAKE J. AGRIC. L. 431, 435 (1997) (quoting Grant Mangold, *How does Global Positioning Really Work?*, SUCCESSFUL FARMING, Feb. 1996, at 14).

¹² Walter, *supra* note 11, at 436 (citing MARK MORGAN & DAN ESS, THE PRECISION-FARMING GUIDE FOR AGRICULTURISTS 10-11 (John E. Kuhar ed., John Deere Publishing 1997)).

¹³ Walter, *supra* note 11, at 436.

¹⁴ *Id.*

a statewide GIS system or clearinghouse,¹⁵ while some state laws relate to freedom of information.¹⁶ The remainder either establish a center for information technology,¹⁷ discuss qualifications for a GIS mapper,¹⁸ or discuss liability.¹⁹

The promise of GIS for sustainable development is great, but this potential continues to be met with growing challenges. Most challenges arise out of homeland security concerns in a post-September 11th era,²⁰ when articles and reports document dozens of instances where federal and state government agencies have

¹⁵ ARIZ. REV. STAT. ANN. § 37-173 (2004); ARK. CODE ANN. § 15-21-504 (West 2004); CAL. GOV'T. CODE § 51017 (West 2004); D.C. CODE ANN. § 50-921.04 (2004); IDAHO CODE ANN. § 58-33-0 (2004); 415 ILL. COMP. STAT § 20/6 (2004); IND. CODE § 2-1-9-10 (2004); IOWA CODE § 446.7 (2004); MASS. GEN. LAWS ANN. CH. 21A § 4B (2004); MINN. STAT. § 466.03 (2004); NEB. REV. STAT. § 86-563 (2004); N.H. ADMIN. R. ANN. § 4-c:8 (2004); N.Y. ENVTL. CONSERV. LAW § 44-0117 (McKinney 2004); N.C. GEN. STAT. § 89C-3 (2004); OKLA. STAT. tit. 82, § 1501-205.1 (2004); OR. REV. STAT. § 196.575 (2004); P.R. LAWS ANN. tit. 25, § 1917 (2004); R.I. GEN. LAWS § 42-11-2 (2004); VT. STAT. ANN. tit. 10 § 122 (2004); WASH. REV. CODE ANN. § 43.63A.550 (West 2004).

¹⁶ CONN. GEN. STAT. § 7-148s (2004); GA. CODE ANN. § 50-29-2 (2004); HAW. REV. STAT. § 92-21 (2004); KAN. STAT. ANN. § 149.338 (2004); MD. CODE ANN., STATE GOV'T § 10-905 (LexisNexis 2004); MICH. COMP. LAWS ANN. § 54.261 (West 2004); MISS. CODE ANN. § 25-61-7 (2004); MO. REV. STAT. § 82.1035 (2004); NEV. REV. STAT. § 239.054 (2004); N.J. STAT. ANN. § 58:10B-23 (2004); N.M. STAT. ANN., § 7-38-9 (West 2004); WIS. STAT. ANN. § 16.966 (West 2004).

¹⁷ ARK. CODE ANN. § 14.40.095 (2004); LA. REV. STAT. ANN. § 1051 (2004); ME. REV. STAT. ANN. tit. 5, § 1881 (2004); TEX. WATER CODE ANN. § 16.021 (Vernon 2004).

¹⁸ COLO. REV. STAT. § 12-25-202 (2004); N.C. GEN. STAT § 89C-3 (2004); OHIO REV. CODE ANN. § 1504.02 (West 2004); S.C. CODE ANN. § 40-22-225 (2004); TENN. CODE ANN. § 4-3-5501 (2004); UTAH CODE ANN. § 63A-6-201 (2004); VA. CODE ANN. 2.2-2025 (2004); W.VA. CODE § 24E-1-1 (2004).

¹⁹ KAN. STAT. ANN. § 75-6104 (2004).

²⁰ See JOHN C. BAKER ET AL., MAPPING THE RISKS: ASSESSING HOMELAND SECURITY IMPLICATIONS OF PUBLICLY AVAILABLE GEOSPATIAL INFORMATION (RAND Corporation, prepared for the National Geospatial-Intelligence Agency, 2004), *available at* http://www.rand.org/pubs/monographs/2004/RAND_MG142.pdf. The report begins: "In the wake of the September 11, 2001 terrorist attacks, U.S. officials have instituted information protection policies aimed at bolstering homeland security. These policies aim to minimize the opportunities of potential attackers exploiting publicly available information they might obtain from federal sources in planning attacks against U.S. homeland locations." *Id.* at xvii.

removed and/or altered spatial data and other related information from their publicly-accessed web sites.²¹ This has presented a growing concern within parts of the environmental community that the government is depriving citizens of their right to know about certain environmental dangers in their communities.²² Making matters worse is the fact that a significant amount of the disappearing data from certain government-sponsored websites was available to the public from either other government websites

²¹ The government did not begin removing data from web sites and other means of public access as a result of September 11, 2001, the practice predates the terrorist attacks. One librarian who has dealt with spatial information for nearly two decades notes that

[e]ven before Sept. 11, 2001, there were a number of reasons why government agencies withheld information from libraries and the public . . . Data availability was limited because of the Cold War, federal legislation protecting certain types of natural and relict human features, Cooperative Research and Development Agreements (CRADAs), exorbitant government information pricing, and the threat of potential terrorism.

Linda Zellmer, *How Homeland Security Affects Spatial Information*, 24 *COMPUTERS IN LIBR.* 4 (2004), available at <http://www.infoday.com/cilmag/apr04/zellmer.shtml>. Zellmer further notes that “[m]uch of the spatial data that has been removed from the Web and libraries contains information regarding critical infrastructure, including water supply, transportation, emergency services, and energy. Access to environmental information has also been curtailed.” *Id.*; see also BAKER ET AL., *supra* note 20, at 1 (“Since the September 11, 2001 terrorist attacks on the U.S. homeland, federal government agencies have withdrawn some data and information that was publicly available before the attacks. These restrictions have included removing geospatial information from Web sites and federal depository libraries.”).

²² See Joseph A. Seigel, *Terrorism and Environmental Law: Chemical Facility Site Security vs. Right-To-Know?*, 9 *WIDENER L. SYMP. J.* 339, 340-41, n.13 (2003) (citing concerns raised by the U.S. Public Interest Research Group at a November 8, 2001, hearing before the Subcommittee on Water Resources and the Environment); see also *The Role of the Public's Right to Know in Increasing Public Safety after September 11th*, Before the House Committee on Transportation and Infrastructure, Subcommittee on Water Resources and Environment, 107th Cong. (2001) [hereinafter Baumann Testimony] (Testimony of Jeremiah D. Baumann, Environmental Health Advocate, U.S. Public Interest Research Group (“PIRG”) and the National Association of State PIRGs), available at <http://www.house.gov/transportation/water/11-08-01/baumann.html>.

or from sites maintained by private and nonprofit entities,²³ putting in doubt the actual security risk posed by an open-access policy. Those who initially decided to withdraw GIS data from public accessibility may have done so under time pressure without allowances for careful study and analysis, and absent guidance from senior-level managers.²⁴ To remain consistent with American societal democratic ideals, however, government must now follow the legal framework that has long promoted public access to government information. Moreover, government must carefully safeguard open access to information that advances the ability of communities to plan for and to protect against environmental and public health concerns.

In 1992, the Rio Declaration on Environment and Development adopted twenty-seven principles and goals of cooperation to strengthen capacity building for sustainable development through the use of both technology²⁵ and full and informed citizen participation.²⁶ Fully informed citizen participation creates “transparency”²⁷

²³ Zellmer, *supra* note 21.

²⁴ BAKER ET AL., *supra* note 20, at 3.

²⁵ U.N. Conference on Environment and Development, June 3-4, 1992, *Rio Declaration on Environment and Development*, Princ. 9, U.N. Doc A/CONF. 151/26/Rev.1 (Vol I) (1993) [hereinafter *Rio Declaration*] (stating that “[s]tates should cooperate to strengthen endogenous capacity-building for sustainable development by improving scientific understanding through exchanges of scientific and technological knowledge, and by enhancing the development, adaptation, diffusion and transfer of technologies, including new and innovative technologies”).

²⁶ *Rio Declaration*, *supra* note 25, Principle 10.

Environmental issues are best handled with the participation of all concerned citizens, at the relevant level. At the national level, each individual shall have appropriate access to information concerning the environment that is held by public authorities, including information on hazardous materials and activities in their communities, and the opportunity to participate in decision-making processes. States shall facilitate and encourage public awareness and participation by making information widely available.

Id. The concept of citizen involvement contained in this principle is central to realizing many of the other twenty-six Rio principles, including achievement of

in government decision-making, “improv[ing] the credibility, effectiveness, and accountability of governmental decisionmaking processes ultimately result[ing] in better implementation of sustainable development objectives.”²⁸ Environmental justice advocates have relied on both government and Internet-provided GIS data to learn about public health and environmental risks present in various minority and low-income communities across the country.²⁹ This very data has now been categorized as meeting the definition of “critical infrastructure” for purposes of planning for homeland security.³⁰ Some believe that due to the aggressive “efforts of cable television and telephone companies to bring . . . cable to their customers . . . large volumes of geographic information could be widely and regularly distributed to the public in [individual] homes before the middle of this decade.”³¹ As long as relevant government-collected information continues to be made

equity, integrated decisionmaking, poverty eradication, unsustainable consumption and precaution. *Id.*; see also Frances Irwin & Carl Bruch, *Public Access to Information, Participation and Justice*, in STUMBLING TOWARD SUSTAINABILITY 511, 512 (John C. Dernbach ed., Environmental Law Institute 2002).

²⁷ Irwin & Bruch, *supra* note 26, at 511.

²⁸ *Id.*

²⁹ See, e.g., Aguilar & Haracz, *supra* note 1 (describing how GIS is used to assist in the analysis of environmental justice issues. Environmental justice advocates integrate the federally provided Toxic Release Inventory with GIS data to assess burdens of industrial air pollution on impacted communities.); see also Seigel, *supra* note 22, at 348.

³⁰ BAKER ET AL., *supra* note 20, at 2 (defining “critical infrastructure sectors” as “agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry and hazardous materials, and postal and shipping”).

³¹ Jack Dangermond, *Sharing Government’s Digital Geographic Information with the Public*, 1 GIS LAW, no. 3, 19-20 (1993). Dangermond, the President of Environmental Systems Research Institute, Inc., a major player in the GIS industry, asserts that “[w]hen [citizens] share more concretely in the fruits of data gathering, they may be more willing to support further development of data gathering; and when they understand problems more clearly, they may be better able to solve them.” *Id.* Dangermond concludes that “we’re at the beginning of an important and beneficial revolution in the use of one kind of government information technology.” *Id.*

public, increased cable access presents an opportunity for a more informed citizenry on myriad environmental sustainability issues.

I. GIS DATA AND THE PROMISE OF SUSTAINABLE DEVELOPMENT

The American Planning Association ("APA") recognizes the importance of GIS as a land use planning tool that "enables governments to more quickly and [accurately] portray, communicate, and analyze existing and potential [environmental] conditions from a visual perspective,"³² thus fostering greater understanding of complex environmental issues.³³ Noting that the general availability of "GIS [data] enables the public and other organizations to be better informed and more effectively involved in the governing process,"³⁴ the APA recommended a model state statute for GIS as part of its Growing Smart effort. Among other things, the model statute calls upon states to establish statewide GIS clearinghouses and geographic information advisory boards, and to address data sensitivity issues so that information is available to the public without compromising needed confidentiality.³⁵ Prior

³² GROWING SMART LEGISLATIVE GUIDEBOOK: MODEL STATUTES FOR PLANNING AND THE MANAGEMENT OF CHANGE 15-3 (Stuart Meck ed., American Planning Association 2002).

³³ *Id.*

³⁴ *Id.*

³⁵ *Id.* at 15-1 to 15-16. The model statute's commentary notes that it is based in part on the existing GIS statutes in Florida, Kentucky, Utah, and Virginia. Other state statutory provisions dealing with GIS include those passed in Arizona, Arkansas, Minnesota, New Hampshire, and Wisconsin. *See, e.g.*, ARIZ. REV. STAT. ANN. § 37-172 (2000), ARK. CODE ANN. § 15-21-501 (2000), MINN. STAT. § 4A.05 (1999), N.H. REV. STAT. ANN. § 4-C:3 (1999), and WIS. STAT. §§ 16.966-16.967 (1999). In July 1997, New York state issued Technology Policy 97-6, which created the NYS GIS Data Sharing Cooperative that "encourages public agencies to share in the creation, use, and maintenance of GIS datasets . . . while providing citizens, the media, and other data users easy access to this resource." James Natoli, Director of State Operations, Governor's Task Force on Information Resource Management, Technology Policy 97-6 (July 17, 1997), http://www.oft.state.ny.us/policy/tp_976.htm.

to September 11, 2001, the debate over the accessibility of GIS data focused on an argument by some in government that the data should not be subject to freedom of information laws primarily because the government was concerned that data collected at the public's expense would be put to private commercial use without adequate compensation back to the government.³⁶ Post-September 11th, federal and state governments appear to be cloaking their reluctance to share certain GIS data by using homeland security as a justification to promote secrecy. In an effort to provide guidance on access to spatial data, the National States Geographic Information Council developed a decision tree to help its members judge whether data should be accessible to the public.³⁷

A. *GIS Information Sharing Policies at the Federal and State Levels*

Noting the critical importance of geographic information in “promot[ing] economic development, improving stewardship of natural resources and protecting the environment,”³⁸ President Clinton issued an Executive Order in 1994 to coordinate geographic data acquisition and access through a coordinated National Spatial Data Infrastructure (“NSDI”).³⁹ “The NSDI assures that spatial data from multiple sources ([all levels of government], academia, and the private sector) are available and easily integrated.”⁴⁰ Among the values NSDI must honor are

³⁶ See, e.g., H. Bishop Dansby, *Commentary: Selling Public GIS Data*, 1 GISLAW, no. 4, 18 (1993).

³⁷ See National States Geographic Information Council, Data Access Decision Tree for Critical Infrastructure Data, July 8, 2002, http://www.nsgic.org/committees/documents/080702_HS_Decision_Tree_CI_Data%20_Version7.ppt.

³⁸ The NSDI was created at the recommendation of the National Performance Review. Exec. Order No. 12,906, 59 Fed. Reg. 17,671 (Apr. 11, 1994).

³⁹ *Id.*

⁴⁰ OFFICE OF MGMT. & BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, OMB CIRC. NO. A-16 Revised § 2 (2002), available at http://www.whitehouse.gov/omb/circulars/a016/a016_rev.html [hereinafter OMB Circular A-16] (providing direction for federal agencies in their maintenance and use of geographic and spatial data); see also *id.* §§ 2b(1-6) (listing the components of the NSDI,

"[a]ccess for all citizens to spatial data, information, and interpretive products,"⁴¹ and the "[i]nteroperability of federal information systems,"⁴² to enable sharing of resources across agency lines.⁴³ Policies developed by the NSDI are applicable to "[a]ll spatial data and geographic information systems activities—financed directly or indirectly, in whole or in part, by federal funds."⁴⁴ One possibly significant limitation on the public access theme is the requirement

particularly "data themes," which are defined as "electronic records and coordinates for a topic or subject, such as elevation or vegetation;" "metadata," which is defined as "information about and/or geospatial services, such as content, source, vintage, spatial scale, accuracy, projection, responsible party, contact phone number, method of collection, and other descriptions;" the National Spatial Data Clearinghouse which provides access to "[a]ll spatial data collected by federal agencies or their agents;" standards, which include the "standards and protocols for data development, documentation, exchange, and geospatial services" and provide that "[n]o federal funds will be used . . . for the development of spatial data not complying with NSDI standards;" and "partnerships" that can occur "among federal, tribal, state, local government, and academic institutions . . . [the] private sector . . . and other business information providers and users").

⁴¹ *Id.* § 2a.

⁴² *Id.*

⁴³ *Id.* OMB Circular A-16 further directs that "international compatibility is an important part of the NSDI." To meet this goal, "[f]ederal agencies will develop their international spatial data in compliance with international voluntary consensus standards" *Id.*

⁴⁴ *Id.* § 6a. The following examples are not meant to be exhaustive, and additional programs may be added at any time, but OMB Circular A-16 indicates that the programs and initiatives covered under its requirements include

[t]he National Mapping Program, the National Spatial Reference System, the National Geologic Mapping Program, the National Wetlands Inventory, the National Cooperative Soil Survey Program, the National Public Land Survey System, Geographic Coordinate Database, the National Oceanic and Atmospheric Administration (NOAA) nautical charting and nautical data collection and information programs, the U.S. Army Corps of Engineers (USACE) inland waterway charting program . . . FEMA's Flood Plain Mapping program and other federal activities that involve national surveying, mapping, remote sensing, spatially referenced statistical data, and . . . [GPS].

Id.

that “[t]he NSDI supports and advances the building of a Global Spatial Data Infrastructure, consistent with national security, national defense, [and] national intelligence”⁴⁵ Executive Order 12,906, as reiterated in OMB Circular A-16, specifically exempts from the requirements of the NSDI

[c]lassified national security-related spatial data activities of the Department of Defense . . . as specifically determined by the Secretary of Defense . . . activities of the Department of Energy, as specifically determined by the Secretary of Energy . . . [and] [i]ntelligence spatial data activities, as specifically determined by the Director of the Central Intelligence Agency.⁴⁶

The FGDC, chaired by the Secretary of the Interior and staffed by the Department of the Interior, is the central “interagency coordinating body for NSDI-related activities.”⁴⁷ All federal agencies that collect, use or disseminate geographic information either internally or through activities involving partners, grants, or contracts, are required to, among other things, publish a

⁴⁵ *Id.* § 2a. The Circular further charges the Federal Geographic Data Committee (“FGDC”) with ensuring “consistency of the NSDI with national security, national defense, and emergency preparedness program policies regarding data accessibility.” *Id.* § 8e(g).

⁴⁶ OMB Circular A-16, *supra* note 40, §§ 7(2), (3).

⁴⁷ *Id.* § 1. The Deputy Director of the Office of Management and Budget is charged with serving as Vice-Chair of the FGDC, and all agencies responsible for spatial data themes are required to participate as members of the FGDC. *Id.* § 4a. As of August 2002, these agencies include: Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, Housing and Urban Development, Interior, Justice, State, Transportation; the Environmental Protection Agency; the Federal Emergency Management Agency; the General Services Administration; Library of Congress; National Archives and Records Administration; National Aeronautics and Space Administration; National Science Foundation; and the Tennessee Valley Authority. OMB Circular A-16, *supra* note 40, at App. B.

strategy for advancing geographic information and spatial data activities in support of the NSDI Strategy.⁴⁸

The E-Government Act of 2002 ("EGA")⁴⁹ reiterates the importance of the collaborative development and use of common protocols for government-sponsored GIS.⁵⁰ As a policy acknowledgment that some GIS data is not shared, the EGA directs that, among other things, common protocols are to "maximize the degree to which unclassified geographic information from various sources can be made electronically compatible and accessible."⁵¹ The EGA further mandates that all federal agencies shall conduct risk assessments and analyses for their various electronic information systems in order to ascertain the potential "harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems."⁵²

A recent report published by the RAND Corporation that addressed public availability of geospatial information about critical sites⁵³ identified "465 [sample data sources representing various federal] programs, offices, or major initiatives at [thirty] different federal agencies and departments,"⁵⁴ but "fewer than [six] percent of [these sites] appeared as though they could be useful to a potential attacker."⁵⁵ Further, "[f]ewer than [one] percent of the . . . datasets . . . examined appeared both potentially useful and unique."⁵⁶ RAND asserts that a combination of usefulness and

⁴⁸ *See id.*

⁴⁹ H.R. 2458, 107th Cong. (2002), § 216(f) (enacted) (authorizing funding through 2007 "[t]o enhance the management and promotion of electronic Government services").

⁵⁰ *Id.*

⁵¹ *Id.* § 216(e)(1). Further, the EGA provides that protocols should be developed to achieve "interoperable" GIS technologies that will allow low-cost and widespread sharing of data across different levels of government and the public. *See id.* § 216(e)(2).

⁵² *Id.* § 3544(a)(2)(A).

⁵³ BAKER ET AL., *supra* note 20, at xxv.

⁵⁴ *Id.*

⁵⁵ *Id.*

⁵⁶ *Id.* at xxv, n.2 (noting that since September 11, 2001, this information is "no longer being made public by federal agencies," as the data has "either been

uniqueness is the appropriate determinant of whether particular geospatial data presents a significant homeland security risk.⁵⁷ Ultimately, the report found that potential attackers have a wide array of avenues through which they can obtain the information required to attack locations within the United States. As a result, “publicly accessible geospatial information is probably not the first choice for fulfilling these needs.”⁵⁸ The report suggests a distinction between information that can be absolutely necessary to a potential attacker, information that is only moderately useful, and information that is not at all essential.⁵⁹ The RAND report also sets forth four recommendations for the federal government’s development of a comprehensive plan for the treatment of sensitive geospatial data, including (1) that “the federal government should play a proactive role in bringing greater coherence and consistency to assessing the homeland security implications of publicly available geospatial information;”⁶⁰ (2) that “[a]n analytical process should be used . . . to assess the potential homeland security sensitivity”⁶¹ of certain geospatial data; (3) that a longer term “comprehensive model for addressing the security of geospatial information” be developed;⁶² and (4) that “the federal government should increase the awareness of the public and private sectors concerning the potential sensitivity of geospatial information.”⁶³

completely withdrawn from public access on the World Wide Web or their agencies have implemented password protection to control access”).

⁵⁷ *Id.* at xxiii.

⁵⁸ *Id.* at xxi. While geospatial data does have the potential to be useful, potential attackers are more likely to obtain information via direct access or observation to better suit their information needs. *Id.* at xxii. The report notes, however, that “we cannot conclude that *publicly accessible* federal geospatial information provides no special benefit to the attacker. Neither can we conclude that it would benefit the attacker.” *Id.* at xxv-xxvi.

⁵⁹ *Id.* at xxii.

⁶⁰ *Id.* at xxxi.

⁶¹ *Id.*

⁶² *Id.* at xxxii.

⁶³ *Id.*

State and local governments rely on federally-developed GIS datasets for their own GIS sharing programs.⁶⁴ In some cases, participant agreements between various governments provide that any records of participating governments that are classified as private or protected from public access are not to be provided to other governments in the GIS cooperative.⁶⁵ These types of agreements, however, may not withstand scrutiny under public access laws in all states. Questions also remain as to who actually owns the data once it is in the possession of governmental entities. The Minnesota Governor's Council on Geographic Information reaffirmed its belief that "the public benefits when governments leverage investments in geospatial data and make it widely available—both to other government units and to the public [T]he council views geographic information as a public resource that should be widely shared and used."⁶⁶

A January 2002 GIS Needs Assessment and Implementation Plan for the State of Maine acknowledged that "[i]n light of general concerns about . . . homeland security . . . protection of privacy will

⁶⁴ See, e.g., North Dakota Geographic Information Systems, <http://www.state.nd.us/gis/resources> (follow "GIS Activities," "GIS Standards" or "GIS Training" hyperlinks for referenced links to federal materials) (last visited Nov. 15, 2005).

⁶⁵ See, e.g., Draft Oregon Digital Spatial Data Sharing and Integration Agreement, State of Oregon and Signatory State and Federal Agencies § 7, http://egov.oregon.gov/DAS/IRMD/GEO/ogic/docs/IGA_Nov04.pdf (last visited Nov. 15, 2005).

Records of the State or its political subdivisions that are classified as private, controlled, or protected under the provisions of Oregon law shall not be provided pursuant to this agreement, unless otherwise available pursuant to Oregon law. Similarly, federal records exempt from release under the provision of the Freedom of Information Act (FOIA), or confidential or proprietary, shall not be provided pursuant to this agreement, unless discretionary authority exists for the exemption.

Id.

⁶⁶ MINN. GOVERNOR'S COUNCIL ON GEOGRAPHIC INFORMATION, MAKING THE MOST OF GEOSPATIAL DATA EXCHANGE: A GUIDE FOR DATA DISTRIBUTION (2003), available at <http://www.gis.state.mn.us/pdf/GeoDataExchange.pdf>.

need to be addressed without undermining the intent of freedom of information statutes.”⁶⁷

B. GIS Can Be an Ally in Promoting Homeland Security

While governments have been focused on the removal of, and restrictions to, certain GIS data because of security concerns, the fact remains that governments are relying on the promise of GIS technology to assist in overcoming homeland security challenges. For example, the GIS Task Force in North Dakota received funding from the Department of Homeland Security to work with the State 911 Association and the Division of Emergency Management on a project to create accurate road centerline information.⁶⁸ Numerous other examples exist of how GIS is being used across the country as a critical tool which enables governments to prevent and prepare for potential environmental hazards.⁶⁹ The FGDC commented that GIS is a valuable tool to assist governments and the public with significant aspects of homeland security including detection, preparedness, prevention, protection, response, and recovery.⁷⁰ When the government significantly restricts public access to important GIS information, however, the public loses the

⁶⁷ APPLIED GEOGRAPHICS, MAINE RESOLVE 23 GIS NEEDS ASSESSMENT & IMPLEMENTATION PLAN 20 (2002), *available at* http://apollo.ogis.state.me.us/sc/final/Final_Report/pdf/Section2.pdf.

⁶⁸ *See Current Status March 15, 2004*, North Dakota Geographic Information Systems (2004), <http://www.state.nd.us/gis/about/status> (follow “March 15, 2004” hyperlink).

⁶⁹ On their website, the FGDC provides several examples of how GIS is being used across the country as a critical tool which enables governments to plan and prepare for potential environmental hazards, including the coordinated application and use of geospatial data in New York City in response and recovery operations following the World Trade Center attack, the development of geospatial data as a foundation for critical infrastructure protection and emergency preparedness and response in the greater Chicago area, and the use of geospatial information to combat and suppress wildfires in the western United States. *Homeland Security and Geographic Information Systems*, Federal Geographic Data Committee, *available at* <http://www.fgdc.gov/publications/homeland.html> (last visited Nov. 15, 2005).

⁷⁰ *Id.*

benefit of being able to plan for any number of potential disasters—whether terrorist activity or another unexpected disaster.

II. PUBLIC ACCESS TO GIS DATA AND HOMELAND SECURITY

Just as some believed that the early policies and procedures of the Bush Administration would have a “far-reaching impact on federal information access,”⁷¹ the events of September 11, 2001, have led to a rapid growth of “information curtailment.”⁷² Commentators note a far greater commitment to government secrecy now than at any other time since World War II.⁷³ Similarly, some commentators question whether the lack of access to public information is based on enhanced security needs or whether it is a case of simple opportunism.⁷⁴ In some cases, government restrictions on public access are being promoted by industry groups based on their self-interested views of critical infrastructure protection.⁷⁵

⁷¹ R. SEAN EVANS & BRAD VOGUS, FEDERAL GOVERNMENT INFORMATION ACCESS IN THE WAKE OF 9/11 (2002), *available at* <http://jan.ucc.nau.edu/~rse/FederalAccess.htm>.

⁷² *Id.*

⁷³ Laura Parker, Kevin Johnson & Toni Locy, *Secure Often Means Secret Post-9/11*, USA TODAY, May 16, 2002, at 1A, *available at* <http://www.usatoday.com/usatoday/20020516/4116384s.htm>.

⁷⁴ *Id.* To be fair, however, even prior to September 11, 2001, the federal government had removed certain spatial data from public access by the military and by Congress (e.g., U.S.G.S. removed cave entrances from topographical maps and information about certain gravesites and archeological sites); *see also* Zellmer, *supra* note 21; Christopher H. Schmitt & Edward T. Pound, *Keeping Secrets*, U.S. NEWS & WORLD REP., Dec. 22, 2003, at 18, *available at* <http://www.usnews.com/usnews/news/articles/031222/22secrecy.htm>.

For the past three years, the Bush administration has quietly but efficiently dropped a shroud of secrecy across many critical operations of the federal government—cloaking its own affairs from scrutiny and removing from the public domain important information on health, safety, and environmental matters . . . Bush administration officials often cite the September 11 attacks as the reason for the enhanced secrecy.

Id.

⁷⁵ *See, e.g.*, ASS'N OF METRO. WATER AGENCIES, STATE FOIA LAWS: A GUIDE TO PROTECTING SENSITIVE WATER SECURITY INFORMATION (2002), *available at*

On October 12, 2001, then-Attorney General John Ashcroft issued a Freedom of Information Act (“FOIA”) Memorandum to all federal department and agency heads superceding the Department of Justice policy memorandum which had been in effect since 1993.⁷⁶ The memorandum calls for a greater degree of agency deliberation when confronted with requests for information.

I encourage your agency to carefully consider the protection of all such values and interests when making disclosure determinations under the FOIA. Any discretionary decision by your agency to disclose information protected under the FOIA should be made only after full and deliberate consideration of the institutional, commercial, and personal privacy interests that could be implicated by disclosure of the information.

<http://www.amwa.net/security/FOIA.pdf>. Executive Director Diane VanDe Hei states that the publication is intended to offer strategies to advocates of amending state statutes so that they provide for FOIA exemptions excluding information from disclosure. The Executive Summary asserts that “transparency in government [through public access laws] exacts a cost. Open access to vulnerability and risk assessments, for example, provides nefarious elements with a road map for attacking the safe, secure, and reliable supply of services from utilities.” *Id.* at Forward (PDF Document at 4).

⁷⁶ Memorandum from Att’y Gen. Ashcroft to Heads of all Fed. Dep’ts and Agencies (Oct. 12, 2001), *available at* <http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm> (last visited Nov. 15, 2005) [hereinafter 2001 FOIA Memorandum]. The Department of Justice (“DOJ”) is charged with overseeing agency compliance with the FOIA, and the DOJ serves as the primary source of FOIA guidance for all agencies. *See* U.S. GEN. ACCOUNTING OFFICE, INFORMATION MANAGEMENT UPDATE ON IMPLEMENTATION OF THE ELECTRONIC FREEDOM OF INFORMATION ACT AMENDMENTS (2002), <http://www.gao.gov/new.items/d02493.pdf> (last visited Nov. 15, 2005) [hereinafter INFO. MGMT. UPDATE]. According to the INFO. MGMT. UPDATE, “[t]he 1993 Attorney General memorandum established an overall ‘presumption of disclosure’ and promoted discretion (when an exemption might otherwise be used to withhold information) to achieve ‘maximum responsible disclosure’ under FOIA.” *Id.* at 10.

In making these decisions, you should consult with the Department of Justice's Office of Information and Privacy when significant FOIA issues arise, as well as with our Civil Division on FOIA litigation matters.⁷⁷

The memorandum adds that when agencies "decide to withhold records, in whole or in part,"⁷⁸ based upon a FOIA request, "the Department of Justice will defend your decisions unless they lack a sound legal basis or present an unwarranted risk of adverse impact on the ability of other agencies to protect other important records."⁷⁹ This new "sound legal basis" standard replaced the "foreseeable harm"⁸⁰ standard, which was employed under Attorney General Janet Reno's 1993 predecessor memorandum.⁸¹ It is believed that the statements contained in this new policy not only "reflect a desire to provide a higher degree of security to

⁷⁷ 2001 FOIA Memorandum, *supra* note 76.

⁷⁸ *Id.*

⁷⁹ *Id.* In response to the 2001 FOIA Memorandum, Senator Patrick Leahy sent a letter to the then-Government Accounting Office ("GAO," now the Government Accountability Office) requesting that they assess the effect of these policy changes on FOIA requests. Letter from Senator Patrick Leahy, Chairman, Senate Judiciary Comm. to the Hon. David Walker, Comptroller General, U.S. General Accounting Office (Feb. 28, 2002), *available at* <http://www.fas.org/sgp/congress/2002/leahy-gao.html> (last visited Sept. 28, 2005). The GAO issued its report in August of 2002, which found a difference in views between FOIA officials and the requestor community about the impacts of September 11th on public disclosure. Subsequent GOA reports found, among other things, that government-wide backlogs in responding to FOIA requests were both substantial and growing. 2001 FOIA Memorandum, *supra* note 75; *see also* HOMEFRONT CONFIDENTIAL: HOW THE WAR ON TERRORISM AFFECTS ACCESS TO INFORMATION AND THE PUBLIC'S RIGHT TO KNOW, (Lucy A. Dalglish & Gregg P. Leslie eds. 2004), *available at* http://www.rcfp.org/homefrontconfidential/Homefront_Confidential_5th.pdf (last visited Sept. 20, 2005) [hereinafter HOMEFRONT CONFIDENTIAL].

⁸⁰ 2001 FOIA Memorandum, *supra* note 76.

⁸¹ *Id.*; *see also* HOMEFRONT CONFIDENTIAL, *supra* note 79 at 61-62 (noting that, with respect to the Ashcroft memo, "[t]he new instruction canceled and replaced a pro-disclosure directive issued in 1993 by then-Attorney General Janet Reno . . . who openly endorsed disclosures of government information").

sensitive information, but just as likely . . . [signal] that agencies are being encouraged to be unresponsive to FOIA requests.”⁸² The Office of Information Privacy within the Department of Justice “followed up on the [Ashcroft memo] with guidance focusing on protection of sensitive material pertaining to vulnerability assessments, safeguard circumventions, and critical infrastructure protections.”⁸³

GIS industry leaders commented that the government rapidly moved in the opposite direction from its pre-September 11, 2001, “open-access society,”⁸⁴ with sites and links being closed temporarily and permanently.⁸⁵ While in some cases the removed information was more likely excessive than actually useful,⁸⁶ in other situations the removal of certain geospatial data could hamper emergency response efforts.⁸⁷ It is estimated that “since . . . Sept. 11 . . . [h]undreds of thousands of public documents have been removed from government Web sites,”⁸⁸ including previously

⁸² EVANS & VOGUS, *supra* note 71, at 4.

⁸³ INFO. MGMT. UPDATE, *supra* note 76, at 11. The report notes that following September 11, 2001, the Information Security Oversight Office within the National Archives and Records Administration, and the Office of Information Privacy within the DOJ “developed additional guidance for reviewing government information regarding . . . homeland security and public safety . . . [by protecting] classified information, previously unclassified or declassified information, and sensitive but unclassified information.” *Id.* at 11-12.

⁸⁴ DATA SECURITY: LOOSE BITS SINK SHIPS, ENGINEERING NEWS-RECORD, Jan. 28, 2002, *available at* <http://enr.construction.com/news/informationtech/archives/020128d.asp>.

⁸⁵ *See id.* Ann Johnson, higher education solutions manager with industry leader Environmental Systems Research Institute (“ESRI”), noted that “[i]mmediately after the attacks, favorite sites on the Internet were closed. Some sites closed pages and links and some were ordered to scrub and even destroy certain assets.” *Id.*

⁸⁶ For example, the Federal Aviation Administration’s web site used to provide “altitude and coordinate information in real-time for airplanes in flight.” *Id.*

⁸⁷ *See, e.g., id.* (noting that by “limiting access to differential GPS data or traffic information” posted by the Federal Highway Administration, for example, could pose “significant issues in many areas for emergency response and construction planning and control people”).

⁸⁸ Parker, Johnson & Locy, *supra* note 73, at 1A. The reporters note that in

available GIS data. The FGDC acknowledges that “[a] great deal of our Nation’s success can be attributed to its openness. Access to information has always been readily available to the American public and they recognize that some risk is acceptable.”⁸⁹ Prior to September 11th, it was widely accepted and understood that government would make GIS databases accessible to the public.⁹⁰

The Homeland Security Act of 2002 (“HSA”) created the position of privacy officer within the Department of Homeland Security to assist with the protection of certain information viewed by the government as confidential.⁹¹ When non-governmental parties voluntarily provide information to the government for use “regarding the security of critical infrastructure and protected systems,”⁹² the HSA requires that the information be permanently exempt from public disclosure,⁹³ denying the public the ability to challenge the veracity of the information and to know what data the government relies upon in its decision-making. Furthermore, even assuming that in the short term there could be a credible need to justify the withholding of critical security information, it is unlikely that it would be subsequently justified to withhold it as permanently classified information just because the provider of the information requested it to be kept private. Despite this pro-privacy bent, other sections of the HSA, such as the Homeland Security Information Sharing Act, acknowledge that even for government to successfully do its intended job under the Act, there is a need for not just federal intra-agency sharing of information, but for intergovernmental sharing among the federal, state, and

addition to information that was removed from the sites, other information was edited and access to some information was made more difficult. *Id.*

⁸⁹ Federal Geographic Data Committee, GUIDELINES FOR PROVIDING APPROPRIATE ACCESS TO GEOSPATIAL DATA IN RESPONSE TO SECURITY CONCERNS (2005), available at http://www.fgdc.gov/fgdc/homeland/access_guidelines.pdf [hereinafter GEOSPATIAL GUIDELINES].

⁹⁰ See, e.g., Harlan J. Onsrud, *In Support of Open Access for Publicly Held Geographic Information*, 1 GIS LAW, no. 1, 3 (1992).

⁹¹ H.R. 5005, 106th Cong. § 222 (2002) (enacted).

⁹² *Id.* § 214.

⁹³ *Id.*

local governments.⁹⁴ The Act acknowledges that “[s]ome homeland security information is needed by the State and local personnel to prevent and prepare for terrorist attack[s]”⁹⁵ and that these needs “must be reconciled with the need to preserve the protected status of such information”⁹⁶ Some of the data included is clearly not only important to governments, but also to citizens in communities that could benefit from information regarding potential environmental targets and hazards in their vicinity, as well as information about various disaster mitigation and security plans.

On March 25, 2003, President Bush issued Executive Order 13,292 (the “Order”) amending a prior Executive Order that dealt with classified national security information.⁹⁷ The Order first acknowledges that the Country’s democratic ideals “require that the American people be informed of the activities of their Government”⁹⁸ and that “our Nation’s progress depends on the free flow of information”⁹⁹ to its people. Nevertheless, the Order states that “the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations.”¹⁰⁰ Reiterating that the protection of “information critical to our Nation’s security remains a priority,”¹⁰¹ the President established within the National Archives an Information Security Oversight Office which shall, among other things, “develop directives for the implementation of this order; oversee agency actions to ensure compliance with this order and its implementing directives; review and approve agency implementing regulations and agency guides . . . [and] convene and chair interagency meetings to discuss matters pertaining to the program

⁹⁴ *See id.* § 891.

⁹⁵ *Id.* § 891(b)(4).

⁹⁶ *Id.* § 891(b)(5).

⁹⁷ Exec. Order No. 13,292, 68 Fed. Reg. 15,315 (Mar. 25, 2003) (amending Executive Order 12,958, which dealt with classified national security information).

⁹⁸ *Id.*

⁹⁹ *Id.*

¹⁰⁰ *Id.*

¹⁰¹ *Id.*

established by this order.”¹⁰² The Order also put into place a revised process for classifying and declassifying information.¹⁰³

A. *Changes in Geospatial Access After September 11, 2001*

After September 11, 2001, government officials were forced “to make decisions about restricting . . . access”¹⁰⁴ to geospatial data under “time pressures,”¹⁰⁵ with little “top-level guidance.”¹⁰⁶ One chronology of disappearing government information post-September 11, 2001,¹⁰⁷ documents dozens of instances of federal government agencies shutting down or restricting public access to information on their web sites.¹⁰⁸ For example, the Department of

¹⁰² *Id.* at 15,327.

¹⁰³ Exec. Order 13,292, 68 Fed. Reg. at 15,328.

¹⁰⁴ BAKER ET AL., *supra* note 20, at xviii.

¹⁰⁵ *Id.*

¹⁰⁶ *Id.*; see also *Right-To-Know after September 11th: Hearings Before the H. Comm. on Transportation and Infrastructure, Subcomm. on Water Resources and Environment*, 107th Cong. (2001), available at <http://www.house.gov/transportation/water/11-08-01/11-08-01memo.htm>. In explaining the purpose of the hearings, the Committee Hearing Report stated that

[f]ollowing September 11, there have been concerns that some information that has been publicly available and widely disseminated may decrease domestic security. On October 2, 2001, the American Water Works Association, representing the water supply community, wrote a letter to President Bush urging “Congress and federal agencies to carefully re-think an appropriate balance between our communities’ right-to-know and domestic security.” On October 3, 2001, the American Chemistry Council wrote to EPA Administrator Whitman to ask that EPA revisit its policies on the public availability of some industry data. “Specifically, we encourage you to take immediate action to temporarily prevent access to off-site consequence analysis (OCA) data as part of the Agency’s Risk Management Plan.”

Id.

¹⁰⁷ Barbara Miller, *Chronology of Disappearing Government Information Data Collected Through October 31, 2002*, <http://tiger.uic.edu/~aquinn/access/chr.html> (last visited Nov. 15, 2005).

¹⁰⁸ *Id.*

Transportation removed pipeline mapping information from its web site, and the Nuclear Regulatory Commission withdrew a map of more than 100 active commercial nuclear reactors.¹⁰⁹ In addition to Internet-based information, the Government Printing Office withdrew access to approximately fifty titles including a CD-ROM produced by the U.S. Geological Survey entitled *Source-Area Characteristics of Large Public Surface-Water Supplies in the Conterminous United States: An Information Resource for Source-Water Assessment*.¹¹⁰

The government has also taken a keen interest in maps and other data assembled by non-government personnel. For example, an architect who created a web site “featuring aerial pictures of nuclear weapons storage areas, military bases, ports, dams and secret government bunkers . . . [was] contacted by the FBI” about the site.¹¹¹ Even a graduate student found his work subject to government scrutiny and classification for mapping the network of fiber-optic cabling throughout the country’s business sectors to satisfy his dissertation requirements.¹¹² In the latter example, the private sector was just as interested in the information as was the government.¹¹³ The work was described by one Department of Homeland Security official as “a cookbook of how to exploit the vulnerabilities of our nation’s infrastructure.”¹¹⁴ The government’s

¹⁰⁹ Seigel, *supra* note 22, at 340.

¹¹⁰ EVANS & VOGUS, *supra* note 71 (citing 1999 U.S.G.S. Open-File Rpt. 99-248).

¹¹¹ Laura Blumenfeld, *Dissertation Could Be Security Threat: Student’s Maps Illustrate Concerns About Public Information*, WASH. POST, Jul. 8, 2003, at A1 (available from LexisNexis; on file with the *William & Mary Environmental Law & Policy Review*).

¹¹² *Id.*

¹¹³ *Id.* When the student presented his findings to the Chief Information Officers of the country’s largest financial services companies, the executives “were ‘amazed’ and ‘concerned’ to see how interdependent their [communication] systems were,” leading them to “plan to simulate a cyber assault and a bomb attack jointly with the telecommunications industry and the National Communications System to measure the impact on financial services.” *Id.* at A6.

¹¹⁴ *Id.* at A6-A7 (internal quotation marks omitted). Brenton Greene, Director for Infrastructure Coordination at the Department of Homeland Security, applauded the student project, maintaining that it should not be “openly distributed.” *Id.* (internal quotation marks omitted).

intense interest in this type of data most likely stems in part from Osama bin Laden's videotaped message of December 2001 urging the destruction of the United States' economy.¹¹⁵

In New York, the Director of the newly-created Office of Public Security issued a confidential memorandum to agency heads and commissioners in January 2002, expressing concern about "a disconcerting amount of potentially compromising information still publicly accessible,"¹¹⁶ and requiring each agency to, among other things, "conduct a review of all sensitive information made available to individuals [and] the public via the agency's Internet site"¹¹⁷ and "via freedom of information [law]"¹¹⁸ requests.

1. Removal of GIS Data

Not long ago, the media documented intentional blurring of some of the U.S. Geological Survey's "highest-quality aerial photographs of [landmarks in] Washington, D.C.,"¹¹⁹ thereby demonstrating the realization of fears about government-limited access to satellite and aerial photography. Ironically, many similar photographs already exist both on and off the Internet, raising serious questions over the effectiveness of such an action. For many analogous reasons, the government's removal of significant GIS data and other information from the Internet may not be achieving intended results. For example, advocacy groups often download databases and post them on non-governmental web sites,

¹¹⁵ *Id.* at A6.

¹¹⁶ Confidential Memorandum from James K. Kallstrom, Director, Office of Public Security, & James G. Natoli, Office of State Operations, to Agency Heads and Commissioners. (Jan. 17, 2001), *available at* <http://www.ombwatch.org/info/2001/inventory1.gif>.

¹¹⁷ *Id.*

¹¹⁸ *Id.*

¹¹⁹ *U.S. Blurs White House, Other Landmarks in Aerial Photos*, USA TODAY, Dec. 24, 2003, *available at* http://www.usatoday.com/news/washington/2003-12-24-blurring-wash_x.htm (noting that the federal government's motivation is "to hide objects in plain view" on the "roofs of the White House, [and] Capitol and Treasury Department," as well as obscure[] aerial "views of the Naval Observatory Compound where Vice President Dick Cheney lives").

allowing the information to be easily accessible to its members and to the public as a whole. These examples demonstrate “the tension that exists between the public’s right to know and security concerns.”¹²⁰

The Bureau of Transportation Statistics removed most publicly accessed GIS data from its web site post-September 11, 2001, explaining that the action enabled the agency to “reevaluate the content available through [its] webpages.”¹²¹ The web pages are now back on-line, presumably with modifications.¹²² “The Department of Energy (“DOE”) removed detailed maps and descriptions of ten nuclear facilities with weapons-grade plutonium and highly-enriched uranium from its website.”¹²³ Similarly, “[t]he International Nuclear Safety Center removed interactive maps [of nuclear plants] from its website.”¹²⁴ “OMB Watch submitted a FOIA . . .

¹²⁰ *Id.* (quoting James Dempsey of the Center for Democracy and Technology) (internal quotation marks omitted).

¹²¹ *See Access to Government Information Post September 11th*, OMB Watch, Feb. 1, 2002, <http://www.ombwatch.org/article/articleprint/213/-/1/1> [hereinafter *Information Post-September 11th*]; *see also Post 9/11 Age of Missing Information*, Clary-Meuser Research Network, <http://www.mapcruzin.com/news/rtkpost911.htm> (last visited Nov. 15, 2005).

The site is a national resource for transportation spatial data and GIS in transportation information. One activist noted that the web site previously indicated that the agency was reviewing the site for security reasons. . . . In response to an email question about why the information was unavailable and when it will return, we received the following: “Due to the attacks on September 11th, BTS [(Bureau of Transportation Statistics)] and all other government agencies have had to reevaluate the content available through our web pages. We do not yet know if this data will be available in the future or if we will permanently offer it only to federal, state and local officials.”

Id.

¹²² *See Geographic Information Services*, Bureau of Transportation Statistics, http://www.bts.gov/external_links/state_gis_resources.html (last visited Nov. 15, 2005).

¹²³ *See Information Post-September 11th*, *supra* note 121.

¹²⁴ *Id.* (“These maps allow users to click on a location of a nuclear power plant to learn more about it.”). The article says the interactive maps referred to in the article were later restored.

request to the Department of Energy (and other agencies) asking what information it removed from its website and what guidelines, if any, were followed to remove the information.”¹²⁵ Immediately following the September 11, 2001, attacks, “[t]he National Imagery and Mapping Agency blocked access to a wide range of its publicly available maps . . . while officials reviewed the maps to make sure they did not contain information that could jeopardize national security.”¹²⁶ The U.S. Air Force base in Tullahoma, Tennessee, reportedly “asked the state to stop taking detailed aerial photographs”¹²⁷ that Tennessee was using to create its GIS.

2. Official Changes in State-Level Policy

Some believe piecemeal amendments to “Freedom of Information laws to reflect technological advances,”¹²⁸ including GIS, are both controversial and unlikely to succeed.¹²⁹ The fact remains, however, that legislative proposals to expand exemptions have been introduced¹³⁰ and passed in “[m]ore than half [of] the

¹²⁵ *Id.*

¹²⁶ Jason Peckenpaugh, *Mapping agency blocks access, postpones outsourcing pact*, GOV'T EXECUTIVE, Sept. 25, 2001, available at <http://www.govexec.com/dailyfed/0901/092501p1.htm>. The National Imagery and Mapping Agency (“NIMA”) “handles mapping and imaging services for the Defense Department and intelligence agencies.” *Id.* While the agency did make most of the maps available shortly after the restriction, maps of U.S. military installations were withheld. Further, “[o]ne intelligence expert questioned the wisdom of [NIMA’s] freeze, noting that since NIMA is not the only source of map information, restricting access . . . will not improve security.” *Id.*

¹²⁷ Homefront Confidential, *A Chronology of Events*, <http://www.rcfp.org/homefrontconfidential/chronology.html> (last visited Nov. 15, 2005).

¹²⁸ Neil Vigdor, *Potential Release of GIS Data Involves ‘Serious Privacy and Security Issues’*, GREENWICH TIME.COM, Nov. 2, 2002, <http://www.mapcruzin.com/news/rtk110802a.htm> (last visited Sept. 26, 2005) (referring to the State of Connecticut situation discussed *infra*).

¹²⁹ *Id.*

¹³⁰ See Parker, Johnson & Locy, *supra* note 73. According to this post-September 11th news account, “[l]awmakers in 18 states [as of 2002, were] examining or [had] passed plans to give local officials more power to shield information.” *Id.*

states”¹³¹ since September 11th. In Arkansas, for example, a new law cited security concerns in amending “the Freedom of Information Act of 1967 to provide exemptions for certain records and meetings concerning public water systems.”¹³² According to one news account, after a county clerk in Iowa received “an unusual request for aerial photographs of a site that includes an Army munitions plant,”¹³³ the legislature approved an effort to classify “architectural drawings for schools, public utilities, airports and some local government buildings.”¹³⁴

In their 2004 Annual Report, the North Carolina Geographic Information Coordinating Council (“NCGICC”) included an appendix listing statutorily restricted data from the statewide GIS site based on confidentiality or security concerns.¹³⁵ The Council

¹³¹ Michael Mariani, *A Little Less Sunshine*, GOVERNING MAGAZINE, June 2004, available at <http://governing.com/archive/2004/jun/foia.txt>.

¹³² Act of Mar. 3, 2003, 2003 Ark. Acts 2487 (expired July 1, 2005), available at <http://www.arkleg.state.ar.us> (follow “Research Resources” hyperlink; then follow “Acts and Bills of Previous Legislative Sessions” hyperlink; then follow “2003 Regular Session Acts” hyperlink; then follow “Search Acts for Specific text” hyperlink; search for “763” under “Act Number”; follow first search result “ACT763”) (providing for FOIA exemptions for records and meetings of the public water systems). The Act, which expired on July 1, 2005, specifically exempts

(15)(A) Records, including analyses, investigations, studies, reports, recommendations, requests for proposals, drawings, diagrams, blueprints, and plans, containing information relating to security for any public water system.

(B) The records shall include:

(i) Risk and vulnerability assessments;

(ii) Plans and proposals for preventing and mitigating security risks;

(iii) Emergency response and recovery records;

(iv) Security plans and procedures; and

(v) Any other records containing information that, if disclosed, might jeopardize or compromise efforts to secure and protect the public water system.

Id. at § 2.

¹³³ Parker, Johnson & Locy, *supra* note 73 at 1A.

¹³⁴ *Id.*

¹³⁵ NORTH CAROLINA GEOGRAPHIC INFORMATION COORDINATING COUNCIL, 2004 ANNUAL REPORT TO THE GOVERNOR AND THE NORTH CAROLINA GENERAL

noted that, “without statutory authority some local governments were making decisions at a technical level to remove certain data sets from their Internet web services because of concerns about terrorism, thus depriving public access.”¹³⁶

A number of states passed new laws that exempt certain information from public access. While most of these statutes do not specifically reference GIS data, the language is broad enough to cover the exempted information in any format, including a geo-spatial representation of the information. For example, since May 2004, a new Alabama law exempts from disclosure information that relates to “security plans, procedures or other security-related information.”¹³⁷ A 2003 Arizona law “prohibits public disclosure of information about drinking water systems.”¹³⁸ A 2004 California law seeks to increase public security by exempting from disclosure information about government efforts to combat security threats, including any information related to facility security that “could be used to aid a potential terrorist . . . attack.”¹³⁹ Similarly, in Georgia, a 2003 law exempts from disclosure “‘any plan, blue print [sic], or other material’ that, if made public, would compromise security.”¹⁴⁰ A new Kansas law “exempts from disclosure records that ‘pose a substantial likelihood of revealing security measures’

ASSEMBLY 18-19 (2004), *available at* <http://cgia.cgia.state.nc.us/gicc/annrep/annrep2004.pdf>. The NCGICC effects cooperation among agencies and the private sector through its thirty-five member council comprised of General Assembly and Governor appointees, state governmental officials, and GIS user committee-elected representatives. Information restricted based on security concerns includes emergency response plans by “[l]ocal [b]oards of [e]ducation . . . [c]ommunity [c]olleges . . . University of North Carolina campuses . . . [p]ublic [h]ospitals . . . [i]nformation technology systems, telecommunications networks, electronic security systems . . . [and] [s]ensitive [p]ublic [s]ecurity [i]nformation . . . [including] details of public security plans and arrangements, or the detailed plans and drawings of public buildings and infrastructure facilit[ies]. . . .” *Id.*

¹³⁶ *Id.* at 4. The council correctly notes that “[t]he larger issue is to determine which data might be ‘useful’ to a potential terrorist.” *Id.*

¹³⁷ HOMEFRONT CONFIDENTIAL, *supra* note 79, at 79.

¹³⁸ *Id.* at 79.

¹³⁹ *Id.* at 80 (internal quotation marks omitted).

¹⁴⁰ *Id.* at 82.

that protect utility, sewer treatment, water and communications systems from criminal terrorism.”¹⁴¹ Another sweeping exemption enacted by Maryland in 2002 authorizes “a custodian to deny access to a public record if access would endanger the public.”¹⁴² A 2002 Illinois law specifically exempts GIS data from the state’s Freedom of Information Law.¹⁴³

The Connecticut legislature entertained, but did not enact, a proposal that would have authorized the division heads of any state agency to “exempt from disclosure any records that they have ‘reasonable grounds to believe may result in a safety risk.’”¹⁴⁴ In 2003, a Connecticut public hearing discussed legislation affecting GIS data, but the proposal received no further action.¹⁴⁵

Voters in Florida amended the state constitution in 2003 to require that any further exemptions from state public access laws require a two-thirds majority in each chamber of the legislature, making it more difficult to further restrict the public’s right to know.¹⁴⁶ California voters in 2004 passed Proposition 59, which “creat[ed] a constitutional right for [the] public to access government information.”¹⁴⁷ In Missouri, a 2004 amendment to the Open Records Law granted “the public broad access to electronic records”¹⁴⁸

3. Federal Geographic Data Committee Offers Interim Guidelines

In September 2004, the FGDC issued interim guidelines for providing access to geospatial data in response to security

¹⁴¹ *Id.* at 83.

¹⁴² *Id.* at 84.

¹⁴³ HOMEFRONT CONFIDENTIAL, *supra* note 79, at 83.

¹⁴⁴ *Id.* at 80.

¹⁴⁵ *Id.* at 81.

¹⁴⁶ *Id.* at 82.

¹⁴⁷ See Propositions: Analysis by the Legislative Analyst, California General Election, Official Voter Information Guide (2004), <http://vote2004.ss.ca.gov/voterguide/english.pdf>.

¹⁴⁸ HOMEFRONT CONFIDENTIAL, *supra* note 79, at 86.

concerns.¹⁴⁹ Acknowledging that “there is not much publicly available geospatial information that is sensitive,”¹⁵⁰ and relying in part on the 2004 study by the RAND Corporation,¹⁵¹ the FGDC guidelines attempt to strike a balance between the public’s right to access government information and the protection of homeland security.¹⁵² Among the guiding principles, the FGDC included the need to “[p]rovide for the free flow of information between the government and the public essential to a democratic society,”¹⁵³ and stated that this information sharing “enables both informed public participation in decision-making and private reuse of government information.”¹⁵⁴

In determining whether certain geospatial data needs to be safeguarded, the FGDC recommends that the agency consider the following factors in making a “user needs assessment” (1) whether the data is “useful for selecting one or more specific potential targets, and/or for planning and executing an attack on a potential target”¹⁵⁵ and (2) whether the information is unique to the data requested.¹⁵⁶ To determine whether the data might be used in planning and executing an attack, the guidelines suggest that the decision-maker consider whether “knowledge of the location and purpose of a feature, as described by the data, have the potential to significantly compromise the security of persons, property, or systems”¹⁵⁷ and whether the data identifies “specific features that

¹⁴⁹ GEOSPATIAL GUIDELINES, *supra* note 89. The guidelines were issued pursuant to OMB Circular A-16, which authorized the FGDC to ensure interagency coordination and to implement the National Spatial Data Infrastructure. *Id.* at 5.

¹⁵⁰ *Id.* at 3.

¹⁵¹ See *supra* notes 53-63 and accompanying text.

¹⁵² GEOSPATIAL GUIDELINES, *supra* note 89, at 3.

¹⁵³ *Id.* In addition, it was recognized that public access to government geospatial information is needed to “enforce laws and regulations for the protection of public health and safety and the environment, land management, and other public purposes.” *Id.*

¹⁵⁴ *Id.*

¹⁵⁵ *Id.* at 1.

¹⁵⁶ *Id.* at 6-8.

¹⁵⁷ *Id.* at 6.

render a potential target more vulnerable to attack.”¹⁵⁸ While guidelines are needed, the reality is that government decision-makers are asked to stand in the shoes of a terrorist to determine whether a person with evil intentions could conceivably use the data to cause harm. For an intimidated American public, it may be too easy to arrive at an affirmative answer. The guidelines attempt to allay this concern by cautioning decision-makers to distinguish between what is sensitive information and what is available by other means. Additionally, the guidelines caution decision-makers “not to automatically assume that the high cost or accuracy of data means that the data [has] high value to an adversary.”¹⁵⁹

When one identifies a security issue, the guidelines direct the decision-maker to determine whether the “security costs outweigh the anticipated societal benefits of active data dissemination.”¹⁶⁰ This is perhaps the most significant determination to be

¹⁵⁸ GEOSPATIAL GUIDELINES, *supra* note 89, at 6. The guidelines further state that decision-makers should consider whether the data:

[P]rovides accurate coordinates for facilities that are not otherwise available and not visible from public locations[;]
[p]rovide[s] insights on choke points, which, if used to plan an attack, would increase its effectiveness[;] [a]id[s] the choice of a particular mode of attack by helping an adversary analyze a feature to find the best way to cause catastrophic failure[;] [and]
[p]rovide[s] relevant and current . . . security-related data that are not otherwise available.

Id.

In determining whether the data would make a target more vulnerable, the guidelines indicate that decision-makers should ask whether the data: “[i]dentify internal features that are critical to the operation of a facility . . . [;] [p]rovide details on facility layout and vulnerabilities such as the location of security personnel or storage areas for hazardous materials[;] [p]rovide insights into operational practices such as shift changes . . . [;] [and] [p]rovide relevant current . . . vulnerability-related data.” *Id.*

¹⁵⁹ GEOSPATIAL GUIDELINES, *supra* note 89, at 7. The guidelines further point out that decision-makers must determine whether the data is unique. While it may be in many cases the only geospatial information that exists about a particular location, if other available reference materials also disclose the same information, then the information would not be unique.

¹⁶⁰ *Id.* at 8.

made. Again, the discretion exercised is not an exact science, and could often lead decision-makers down the path of non-disclosure.¹⁶¹ For example, the guidelines instruct the decision-maker to consider whether "sensitive information [would] cause security costs such as: [a] significant increase in the likelihood of an attack[;] [a] significant decrease in the difficulty of executing an attack[; and a] significant increase in the damage caused by an attack."¹⁶² If the answer to any of these inquiries is yes, then a decision-maker must determine whether the "anticipated security costs outweigh the anticipated societal benefits,"¹⁶³ including: "Continued or increasing effectiveness of public health and safety[;] [c]ontinued or increasing support of legal rights (for example, 'right to know')[;] [and] public involvement in decision-making."¹⁶⁴ In ascertaining whether to 'safeguard data' (e.g., deny public access) when the security risk could outweigh the benefit of dissemination, the FGDC states that 'safeguarding' is only justified if the sensitive information is unique to the data source.¹⁶⁵ It follows that much of the GIS information removed from government websites in the weeks following September 11th was likely

¹⁶¹ See EVANS & VOGUS, *supra* note 71. Two librarians noted in their review of changing tides in government access policies that:

Clearly, the events of 9/11 have caused the government of the United States as a whole to think about information access and related policies. It is obvious that federal information . . . has the potential for use against the United States by foreign or domestic terrorist groups or individuals, and as such the federal government re-evaluating access and distribution policies makes a degree of sense. The problem with such a philosophy is making the determination as to what exactly constitutes harmful information. In other words, while few would argue the merits of curtailing certain forms of information, the uncertainty as to just what sort of publications and Web sites will constitute "dangerous" information leaves the impacts of these actions unpredictable.

Id.

¹⁶² GEOSPATIAL GUIDELINES, *supra* note 89, at 8.

¹⁶³ *Id.*

¹⁶⁴ *Id.*

¹⁶⁵ *Id.* at 9.

not justifiable since much of the data was no longer unique to the primary web source due to downloads, copying, and republication by others.

Where a decision-maker reaches the conclusion that certain geospatial data has elements that justify safeguarding, the FGDC recommends that the agency consider whether changing the data (for example, the “redaction or removal of sensitive information and/or reducing the sensitivity of information by simplification, classification, aggregation, statistical summarization, or other information reduction methods”) sufficiently safeguards it so that other useful aspects of the information could remain accessible.¹⁶⁶ If a decision-maker determines changes are appropriate, the agency should “document the changes using the metadata.”¹⁶⁷ This reasonable approach favors at least some level of disclosure over no disclosure at all. Much data within GIS generated maps, for example, can be extremely useful to environmental advocates and the public, without including all layers of available detail that might compromise short-term security needs. Finding appropriate ways to share as much information as possible on a timely basis, albeit by withholding certain aspects or layers of data, can advance the public’s right to know, especially when the agency identifies withheld information and validly justifies any nondisclosure.

¹⁶⁶ GEOSPATIAL GUIDELINES, *supra* note 89, at 9. The FGDC notes that it is important to determine whether the agency has the authority to change the data (e.g., “laws, regulations, policies, or concerns about liability may compel [the organization] to [simply] release data”). *Id.* at 10. The FGDC further notes that where a decision-maker is uncertain about the agency’s authority to change data, they should seek a “policy decision” from that agency’s management or legal counsel. Additionally, the FGDC recommends that agencies have “written procedures and policies describing the types of changes” that are authorized “and the conditions under which [these actions will be] permitted.” *Id.*

¹⁶⁷ *Id.* at 9. The FGDC suggests

[f]our types of information should be encoded in metadata: (1) the fact that the geospatial data and metadata were reviewed using the guidelines, (2) decisions that were made, (3) the date[s] of the decisions, and (4) the safeguards (changes to the geospatial data or restrictions on access, use, or dissemination of the geospatial data and metadata) that were applied.

Id. at 14.

The FGDC also suggests that agencies may wish to establish different “levels of restriction [to] geospatial data.”¹⁶⁸ For example, the agency may determine that certain data must be

[g]enerally available to members of the public with use and redistribution restrictions. Recipients may be required to identify themselves before receiving the geospatial data[;] available to other government agencies or non-governmental organizations (for example, the Red Cross), with use and redistribution restrictions[;] available only to law enforcement, first responder, and emergency management agencies with use and redistribution restrictions[;] available only to “partner” agencies from other levels of government with use and redistribution restrictions[; and] available only within your organization.¹⁶⁹

B. *GIS Access and the Courts*

Current litigation is making its way through the Connecticut courts after the Town of Greenwich denied a request to provide a member of the public with an electronic copy of certain information contained in the town’s GIS database.¹⁷⁰ The three million dollar database contains, among other things, computer records containing aerial photographs, road and sewer maps, and property assessment data.¹⁷¹ In January 2004, the Superior Court of Connecticut upheld a State Freedom of Information Commission decision ordering the town to comply with a citizen’s request for a copy of the GIS database.¹⁷² In defending its denial of the request,

¹⁶⁸ *Id.* at 11.

¹⁶⁹ *Id.*

¹⁷⁰ Dir., Dep’t of Info. Tech., *Greenwich v. Freedom of Info. Comm’n*, 36 Conn. L. Rptr. No. 9, 338, 2003 Conn. Super. LEXIS 3617 (New Britain 2003); *see also* Ivan H. Golden, *News Groups Back Release of Town Data*, GREENWICH TIME, Nov. 10, 2004 (on file with the *William & Mary Environmental Law & Policy Review*).

¹⁷¹ Golden, *supra* note 170.

¹⁷² *Freedom of Info. Comm’n*, 36 Conn. L. Rptr. No. 9, at 338-39. The citizen

the town relied on the testimony of its Chief of Police and argued that the “release of the GIS database would result in the assistance and facilitation of criminal and/or terrorist activities.”¹⁷³ Finding “no nexus between [the Chief of Police’s] opinion and the ultimate” request denial, the court noted that no statistical data offered would correlate to an increase in criminal activity or potential terrorist type activity with disclosure of GIS data.¹⁷⁴ The court warned that “[a]nxiety concerning public safety should not become a canard for creating an exemption”¹⁷⁵ from the requirements of public access.

III. DEVELOPING A SUSTAINABLE POLICY FOR GIS INFORMATION

In an era of public fear of another terrorist attack, the government has led the American public to believe that a choice must be made between effective homeland security and the right to access government information.¹⁷⁶ As one leading environmental health advocate explained, however, “[t]he right to know should

submitted a FOIA request for “all [of] the GIS database pertinent to orthophotography, Arc Info coverages which is a GIS software program, sequel server which is a database format that houses the tax assessment records, and all documentation created to support and define coverages for the Arc Info data set.” *Id.* The court noted that the “complainant carefully requested those portions of the GIS database pertinent to orthophotography and tax assessments, which are public records, and not the entire contents of the GIS database[,] which includes additional information that may not be for public disclosure.” *Id.* at 340.

¹⁷³ *Id.* at 339-40.

¹⁷⁴ *Id.* at 340.

¹⁷⁵ *Id.*

¹⁷⁶ See, e.g., Baumann Testimony, *supra* note 22 (Baumann stated that “[u]nfortunately, some industry interests that have consistently opposed public disclosure of the dangers they pose to neighboring communities have attempted to frame the discussion of how to address this problem by pitting the public’s right to know against the need for national security.”); see also Parker, Johnson & Locy, *supra* note 73, at A1. Gary Bass, executive director of OMB Watch, stated that “[w]e seem to be shifting to the public’s need to know instead of the public’s right to know.” *Id.* (internal quotation marks omitted).

not be considered a threat to national security or public safety.”¹⁷⁷ The advocate further argued that restrictions on the public’s right to know, particularly the public’s right to environmental and public health data, will hurt public safety rather than protect it.¹⁷⁸ Even the federal government acknowledges that GIS technology is critically important to helping the country meet its homeland security goals, noting that “[t]he current state of geospatial information technology can provide decision-makers the data they need to confidently confront a wide variety of threats including natural disasters, terrorist attacks, sabotage, and similar crises.”¹⁷⁹ In its fiscal year 2003 Annual Report, the FGDC noted a continuing need for “a clear, concise and enforceable policy regarding the classification, privacy and proprietary nature of certain types of geospatial data”¹⁸⁰ relative to homeland security. The Working Group Summary Report¹⁸¹ contained in the annual report acknowledged that “homeland security data is faced with differing views on what constitutes sensitive data and the conflicting desires to

¹⁷⁷ Baumann Testimony, *supra* note 22.

¹⁷⁸ *Id.* Baumann maintains that:

Choosing restrictions on the public’s right to know about hazards in communities, rather than actually reducing those hazards, can hurt safety rather than help it. By restricting our right to know, even through a well-intentioned effort to protect [public] safety, government is abandoning its duty to warn the public if a community is at risk.

Id. Baumann also notes in his testimony that restricting the public’s right to know prevents the public from participating in either the prevention of a terrorist attack or the preparation of appropriate response plans. *Id.*

¹⁷⁹ FGDC White Paper, *supra* note 69. The FGDC notes that “[a]s the concept of Homeland Security becomes infused into the work-a-day pattern of government and the everyday life of our citizens, decision makers [sic] will greatly profit from the crisis management ‘edge’ that GIS provides.” *Id.*

¹⁸⁰ FED. GEOGRAPHIC DATA COMM., ANNUAL REPORT SUMMARY (2003), available at <http://www.fgdc.gov/03nsdi/summaries/narrative.pdf>.

¹⁸¹ FED. GEOGRAPHIC DATA COMM. ANNUAL REPORT TO OMB (2003), available at http://www.fgdc.gov/03nsdi/workinggroups/HSWG_2003_Annual_Report.pdf. The Homeland Security Working Group (“HSWG”) is a subcommittee of the Federal Geographic Data Committee. The report is a directive to Agencies on the format for their Annual Spatial Data Reports.

protect sensitive information and to allow for broad participating in processes, data development, and sharing.”¹⁸²

An effective and reasonable public policy promoting public access to GIS data and should have the following elements (1) uniform laws to help state and local governments design and implement appropriate public access policies for GIS data, (2) clear criteria to assist government decision-makers in their determination of whether to grant public access requests for GIS data, and (3) consistent interpretation and enforcement of these laws across agencies at the same level of government. Furthermore, state and local governments must partner in the development of GIS information sharing policies because these government assemble and maintain so much of the relevant and critical data for local community sustainability.¹⁸³

The RAND report suggests an appropriate framework for assessing the potential risks posed by publicly accessible GIS through the following three-part inquiry into the decision-making

¹⁸² FED. GEOGRAPHIC DATA COMM., WORKING GROUP REPORT SUMMARY (2003), available at http://www.fgdc.gov/03nsdi/summaries/working_group.pdf. The HSWG further noted that

[a] unique factor added by homeland security applications is the need for confidentiality for some information and processes. Challenges in this area include different views regarding what is sensitive and authorities for protecting information, and contradictions between the need to restrict access to information and to provide for broad participation in processes and data development and sharing.

FGDC ANNUAL REPORT TO OMB, *supra* note 181.

¹⁸³ BAKER ET AL., *supra* note 20. According to the RAND report, [s]tate and local governments use critical site geospatial information to improve their operations and the services that they supply to the public. For instance, they use geospatial information about such features as water systems, utilities, hazardous chemical sites, road systems, and property ownership to maintain, inspect, regulate, and operate community infrastructure and facilities; to prepare for emergency response, transportation, and other community planning; and for other purposes.

Id. at 55.

analysis involving (1) whether an attacker would find the information useful, (2) whether the information is unique, and (3) “the societal benefits and costs of restricting public access”¹⁸⁴ to particular data. The FGDC’s interim guidelines closely track the RAND protocols, offering further discussion and analytical frameworks for decision-makers. So many different individuals, including career civil servants and political appointees, exercise discretion in determining the accessibility levels of various GIS datasets. For example, those who decide whether to post information to the agency website in the first instance are likely different from those who will respond to a FOIA request for the data. It is likely that no uniformity of results exists across agency lines. Furthermore, but for the RAND report and the interim guidelines that appear to set forth a roadmap for disclosure, federal policy still weighs more heavily in favor of nondisclosure over public accessibility, as evinced by Ashcroft’s support for decision-makers’ leanings towards nondisclosure.

The federal government is not the only public source of important government GIS data. State and local government policies have not seen the scrutiny of a similar RAND-type study¹⁸⁵

¹⁸⁴ BAKER ET AL., *supra* note 20, at xxvi. The RAND report suggests key questions that could be asked for each of these factors. To determine usefulness, the decision-maker should ask whether “the information [is] useful for target selection or location purposes . . . [or] for attack planning purposes.” *Id.* at xxvii. To determine uniqueness, decision-makers should consider whether “the information [is] readily available from other geospatial information sources . . . [or] from direct observation or other information types.” *Id.* Lastly, to assess the societal benefits and costs, decision-makers should consider “the expected security benefits of restricting public access to the source . . . [and] the expected societal costs of restricting public access.” *Id.*

¹⁸⁵ BAKER ET AL., *supra* note 20, at 58-59. The RAND report noted that after September 11th,

some state and local governments [were] restricting public access to geospatial information . . . [h]owever, which governments restrict and what they restrict appear to be inconsistent . . . [s]uch inconsistencies among nonfederal entities in restricting public access is another reason why a federal analytical process is needed to assess and identify potentially sensitive information by providing state and local governments

and no national intergovernmental coordinating body exists to provide technical assistance, training, and education for government decision-makers on these issues. National standards must be developed for application across governmental jurisdictions. A government-university partnership should convene a national summit with representatives from all levels of government and academia. Individual attendees should include GIS professionals, security specialists, and public access officers. In addition, representatives of non-profit advocacy organizations, such as environmental and public health advocates, must participate in the discussion and development of policies to ensure balance of clear justifications for the withholding of government GIS data with the public's right to know.

The White House and the Department of Justice must concurrently re-examine post-September 11, 2001 policies that may support and promote even the *appearance* of secrecy in government, if not the reality thereof. State and local governments should likewise conduct similar intra-governmental assessments and take necessary steps to re-open access to GIS data.

CONCLUSION

In the aftermath of September 11, 2001, the message to Americans from the public and private sector leadership was that the country must continue with business as usual and that deciding not to travel, not to participate in large public gatherings, and to alter any other part of their typical daily routines would signal that the American people were affected by terrorism.

The reverse is true as well. The government must not continue to withhold important environmental and public health related GIS data in response to a terrorist event or the threat of further terrorist activity. Doing so compromises important values of our democracy, including government accountability to the

a federal model that they can use in developing their own approaches.

Id.

people and an open and honest communication between the government and the people. While many may have understood the immediate post-September 11 reaction that produced such an unprecedented shut-down of many information pipelines, these quick reactions should have been temporary in nature, a brief moratorium of sorts. Now that four years have passed, it is time to re-open the flow of facts and figures. Achieving a sustainable environment is dependent upon the ability of the community to access relevant, accurate and timely information from its federal, state, and local governments.