

Policy Review: Blocking Public Geospatial Data Access Is Not Only a Homeland Security Risk

R. Bradley Tombs

Abstract: *This is a policy review of current public geospatial data dissemination practices and the Federal Geographic Data Committee (May 2004) guidelines for geospatial data access. It evaluates if the federal guidelines give proper weight to the societal benefits of record dissemination, the importance of informed citizenry, and its strong Constitutional connection to petition government to redress grievances. Practical examples of state and local policies are exposed, disclosing the conflicts with the federal National Map program objectives. Homeland security and other public risks associated with nondisclosure of public record geospatial records are identified. The review shows that slow progress is being made in bringing order to public geospatial records disclosure, but ill-informed record holders unduly delay access, causing weakness in homeland security preparedness.*

Current Public Geospatial Data Dissemination and Access

Is an informed citizenry important to a homeland security defense to vigilantly protect resources, facilities, and freedoms? If the foundation of a democracy is to have an informed citizenry, it is important to question efforts that block access to nonclassified geospatial data. There is concern that current record access policies and practices are a precursor to secrecy legislation, an uninformed citizenry, and increased homeland security risks. This is a policy review of current public geospatial data dissemination practices and the Federal Geographic Data Committee (FGDC) guidelines for geospatial data access.

After terrorists attacked the Pentagon and the World Trade Center buildings, most government agencies hastily withheld map data and other records from the public, thus curtailing citizens' ability to inform themselves. Everything from hazardous-waste sites to water-main locations are now being considered "possible terrorist targets" by record custodians and map data showing their locations are subjectively deemed a "homeland security" risk. Indeed, impeding federal Freedom of Information Act (FOIA) and State Public Record Act access significantly affect citizens' ability to inform themselves and "to petition the Government for a redress of grievances" afforded by the U.S. Constitution.

Some agencies still attempt to assert that geospatial data are not even public records. Legal cases at both the federal and state levels have nearly ended that assertion, which is now codified by many state public record acts and the FOIA. Key legal cases and documents include: *Petroleum Information Corporation v. U.S. Department of Interior*, 1992; *Delorme Publishing v. NOAA*, 1995; *Higg-a-rella v. Essex County*, 1995; *Drummond v. City of Bellevue*, 1996; and Office of Management and Budget Circular A-130. Improper practices include attempts to charge a fee for a government record beyond the cost of reproduction, which impedes access by diminishing one's ability to redress government on public matters. Federal agencies are even denied state and local

records by agencies seeking to improperly recoup geospatial data development costs.

Three years after the 9/11 attacks, geospatial public records access remains uncertain. Rand Corporation's National Defense Research Institute published *Mapping the Risks, Assessing the Homeland Security Implications of Publicly Available Geospatial Information* (2004). The FGDC Homeland Security Working Group, administered by the Office of Management and Budget (OMB), published *Guidelines for Providing Appropriate Access to Geospatial Data in Response to Homeland Security Concerns*. Although these titles may imply efforts aimed toward restricting nonclassified geospatial record access for fear of use by nefarious individuals, they expose that most data sets do not pose a homeland security risk. The FGDC guidelines generally define "sensitive information" or more precisely what is not sensitive. Secondly, the process considers the "societal costs of limiting public access." Notwithstanding, record custodians are ambiguously placing emphasis on undefined "potential" and "possible" risks to "sensitive" or "critical infrastructure" in prohibiting public spatial data access. While deliberating what records are "sensitive" and "who" should be prohibited access, record custodians are improperly using the "homeland security" excuse to ignore record access laws.

For example, New Jersey's Executive Order #21 seeks regulations to exempt records from the Open Public Record Act that would "substantially interfere" with the state's ability to protect against acts of terrorism or materially "increase the risk" of "potential acts" of sabotage. Inasmuch as the range of potential risks is more or less unlimited, the executive order's indefinite language would lead to ambiguous record restrictions. Should this allow a water utility agency to assert that its water mains are "critical infrastructure" and be entitled to block access to its entire map data although the information is customarily accessible? It would be plausible for Machiavellian officials to route a pipeline through a political friend's farmland, funnel inflated property acquisition

money, and use the spurious “homeland security” excuse as the reason to avoid public scrutiny. The opportunity for public officials to use the terrorism and homeland security excuse as a shield to block records access becomes a dangerous risk itself.

Misused Terminology

This broad executive order language is already used by record custodians to thwart public spatial data access, despite no evidence of any spatial data use risk. The New Jersey’s Domestic Security Preparedness Task Force 2003 annual report uses the term critical infrastructure 40 times, with select examples (e.g., oil/chemical facilities, bridges, tunnels, power plants, national monuments, airport, Hudson River crossings, and “other critical infrastructure sites”). In all cases, the protection of critical infrastructure is stated in a context of assessing a “site’s specific vulnerabilities,” “increasing physical security of the facility,” “developing capacity and specific plans to respond to a crisis,” and “preparing contingency and continuity plans.” Not once does the report specify any restrictions to spatial map data or identify maps or map data as critical infrastructure, at-risk documents, classified, or confidential. Also, the report uses the term Geographical Information Systems (GIS) seven times in the context of integrating GIS into all homeland security efforts for response preparedness.

The misuse of the term critical infrastructure is the default excuse from state and local agencies in the withholding of spatial map records ordinarily available to the public. This spurious excuse perhaps originated with the passing of the Critical Infrastructure Information Act (2002), a subtitle of the Homeland Security Act. At issue are the definitions of critical infrastructure, voluntary, and confidential. Critical infrastructure as defined in the Patriot Act involved “systems and assets” “so vital” that their “incapacity or destruction would have a debilitating impact” on “national economic security.” The Homeland Security Act clarified “critical infrastructure information” as “not customarily in the public domain,” nor information otherwise required for a federal license, permit, grant, etc. Critical infrastructure information does include “voluntary” submissions to the Department of Homeland Security when accompanied by an “express statement” expecting protection from disclosure. It also requires the record holder to certify that the record is “confidential” and not customarily made available to the public.

Critical Infrastructure

Whether the Homeland Security Act created a new or perceived “critical infrastructure,” FOIA exemption is debatable. FOIA exemption 4 already protected against trade secrets and confidential disclosures, which could include “voluntary” critical infrastructure material. *Critical Mass Energy Project v. NRC* is recognized as establishing the test to determine “confidential” information, ruling that voluntarily submitted information is exempt from disclosure under FOIA if the submitter can show that it does not customarily release the information to the public (Stevens February 2003). The Procedures for Handling Critical Infrastructure

Information, Interim Rule, requires that “The information is of a type not customarily in the public domain” (6 CFR Section 29.5 (a)(iv), February 20, 2004).

The Presidential Directive on Critical Infrastructure Identification, Prioritization, and Protection (December 17, 2003) recognizes that most critical infrastructures resources are owned by private sector and state or local governments. The policy in carrying out this directive requires the appropriate handling of “voluntarily” provided information that would facilitate terrorist targeting of critical infrastructure, and directs policy implementation in a manner consistent with applicable provisions of the law, “including those protecting the rights of U.S. persons.” The Homeland Security Act does not preempt state disclosure laws. Although it could be technically argued that there is a new FOIA “critical infrastructure” exemption relating to homeland security, the change appears relatively immaterial for records in general, and not material to geospatial data from a practical records access perspective.

At the same time that many government record holders are strategizing how to conceal public records, the state and federal agencies are working on the federal National Map program to compile GIS geospatial data for public disclosure as a means of response preparedness. Michael Domaratz, Cochair of the Federal Geographic Data Committee (FGDC) Homeland Security Working Group, said, “The map will be in the public domain, and the public will have round-the-clock access” (Sietzen 2004). Presidential Executive Order 12906 stipulates public access to geospatial data, and it is currently available at <http://www.nationalmap.usgs.gov/>. But local public agencies are withholding GIS information. Domaratz questions, “In the event an incident happens . . . how can we access the [local] data?” Denying local map data to the federal government and public could cause delays in responding to catastrophic attacks, a problem noted on 9/11. Unmistakably, local governments that cloak spatial data records can create a public and homeland security risk.

At the same time New Jersey’s executive order language is being used to block public access to spatial data, the New Jersey’s Office of Geographic Information Systems (OGIS) has agreed to provide its spatial data to the FGDC for the National Map program. The OGIS, in the Office of Information Technology, is part of the Domestic Security Preparedness Task Force. One can reasonably deduce that if the federal government’s FGDC and state’s specially created task force are working together to make geospatial data available to the public, local agencies are logically remiss in withholding their records.

Societal Benefits

Prior to 9/11, the societal benefits of government records were not in question. Now, even the Rand report in asserting that “assessing the societal benefits and costs of restricting public access to geospatial information is not straightforward” subtly understates a fundamental principle of our democracy. Citizens’ constitutional right to redress their government is materially weakened

if citizens are denied government records on matters of public concern. Congress recognized its obligation to make government information accessible to citizens by establishing the Government Printing Office (GPO) in accordance with Congressional Joint Resolution 25 of June 23, 1860. OMB Document A-130 details FOIA objectives and procedures, indicating that other nations “do not share [our] values” concerning freedom of information and government records access. The purpose of government in “disseminating the information in the public interest” is straightforward and unambiguous. Understating the importance of records access as integral to our fundamental democracy principle, the need for an informed citizenry, and its close Constitutional connection to citizens’ right to redress government of grievances would be a significant material omission.

Perhaps not as highly prioritized as warranted, the Rand report and FGDC guidelines do integrate the legal principles of our Constitution by weighing “societal benefits and costs.” In presupposing that a data set is “conceivably sensitive” and whether “public access should be curtailed in some way” gives undue credence to an unnecessary analytical process that can delay records access. Most, if not all, nonclassified “conceivably sensitive” records lack the teeth to stand up to legal scrutiny of the “societal [Constitutional] benefits” test. But use of an analytical process by ill-informed (or pressured) record custodians can delay access by gumming to death citizens seeking to be informed. A more than minor delay in records access is a legal defeat of our fundamental democracy principle. Conversely, a timely informed citizenry will best enable homeland security agencies to thwart potential attacks and be responsive in the event of an attack.

Denying spatial record access poses risks beyond diminished public vigilance and response preparedness. It is almost unbelievable that the importance of public record access and free speech rights on matters of public concern is being ignored at many government levels. The Rand report and FGDC guidelines should significantly help to restore some semblance of logic to the hastily withdrawn data by many government agencies. The FGDC rationally indicates that most geospatial data is not sensitive; “sensitive information does not include the fact of the existence of a facility at a particular place or the general layout of a facility.” Rather, it suggests that “attribute data are more likely to be sensitive than geospatial data.” But even the argument that attribute data might be sensitive must withstand the “societal benefit” test that obligates citizens to be informed and redress government of grievances on matters of public concern. In a legal and practical context, public spatial data should either be federally “classified” or made publicly accessible. The FGDC guidelines are a good first step in making that case.

About the Author

R. Bradley Tombs received a Master of Environmental Science degree from Miami University (1984) and a Bachelor of Science degree from Davis & Elkins College (1982). He has

worked in the engineering and environmental consulting industry for 20 years, primarily on behalf of government entities. Tombs has been actively involved in public record geospatial data access issues for nearly ten years and actively volunteers to assist local community groups on matters of public concern.

Corresponding Address:
319 Laurel Court
Point Pleasant Beach, New Jersey 08742
btombs@pngusa.net

References

- Attorney General Ashcroft’s FOIA Memorandum, October 15, 2001.
- Baker, J. C., B. E. Lachman, D. R. Frelinger, K. M. O’Connell, A. C. Hou, M. S. Tseng, D. Orletsky, and C. Yost. 2004. Mapping the risks, assessing the homeland security implications of publicly available geospatial information. Rand, National Defense Research Institute.
- Code of Federal Regulations, February 20, 2004, Part IV, Department of Homeland Security, Procedures for Handling Critical Infrastructure Information; Interim Rule, 6 CFR Section 29.5 (a)(iv) 69(34): 8073-89.
- Federal Geographic Data Committee, <http://www.fgdc.gov/>.
- Federal Geographic Data Committee. Public review version, Guidelines for providing appropriate access to geospatial data in response to security concerns. (Reston, VA: U.S. Geologic Survey, May 3, 2004).
- Homeland Security Act of 2002.
- Homeland Security Presidential Directive, December 2003. Management of federal information sources. Office of Management and Budget Circular A-130.
- McGreevey, Governor James E. Executive Order #21, State of New Jersey.
- National Map, <http://nationalmap.usgs.gov/>.
- New Jersey Domestic Security Preparedness Task Force. 2003 Annual Report, New Jersey. Perritt, H. H., Jr. Should local governments sell local spatial databases through state monopolies? *Jurimetrics Journal* 35(1995):449-69.
- Presidential Executive Order 12906. April 13, 1994. Amended by Executive Order 13286. March 5, 2003. Coordinating Geographic Data Acquisition and Access: The National Spatial Data Infrastructure, <http://www.fgdc.gov/>. Sietzen, F., Jr. October 1, 2003. Federal GIS: a weapon of mass dysfunction? *Geospatial Solutions*, <http://www.geospatial-online.com>.
- Stevens, G. M. February 28, 2003. Homeland Security Act (HSA) of 2002: Critical Infrastructure Information Act. Congressional Research Service, The Library of Congress.
- The USA PATRIOT Act of 2001.