Access to Geographic Information: Openness versus Security

Professor Harlan Onsrud
Department of Spatial Information Science and Engineering
University of Maine
Orono, Maine
Onsrud@spatial.maine.edu

Notice: The following is a preprint version (August 2002) and may differ substantially from an article that ultimately appeared as Onsrud, H.J., 2003, Access to Geographic Information: Openness versus Security. In Cutter, S., D. Richardson and T. Wilbanks (Eds.), Geographic Dimensions of Terrorism (Routledge).

Introduction

One month after the attacks of September 11, 2001, government depository libraries across the U.S. received a request from the U.S. Geological Survey through the Library Programs Service of the U.S. Government Printing Office to destroy copies of a compact disk titled "Source-Area Characteristics of Large Public Surface-Water Supplies in the Coterminous United States: An Information Resource for Source-Water Assessment, 1999." Similar instructions to hold back or destroy wide-ranging materials previously accessible to the general public were issued within and among local, state and U.S. federal government agencies and are presumably continuing today. The requests and directives are being made under the reasoning that certain information in openly published or accessible documents might provide information of value to terrorists. Questions arise as to whether some of the withholdings, even if legal, support rationally the goal of increasing the security of communities and the nation. This article raises the question of whether a general climate of restricting public access to geographic and related data may actually jeopardize rather than increase homeland security.

Some Legal Issues regarding Access

The purpose of the U.S. Freedom of Information Act (FOIA) (USCS Title 5 § 552) is to require federal agencies to make agency information generally available for public inspection and copying for any public or private purpose. Congress has declared that the act has resulted over time in a valuable means through which any person can learn how the government works, has led to the disclosure of waste, fraud, abuse and wrongdoing in the Federal Government, and has led to the identification of unsafe consumer products, harmful drugs, and serious health hazards (for instance, see HR 3802, Electronic Freedom of Information Act Amendments of 1996, http://www.epic.org/open-gov/efoia.html). Other assessments indicate that the current deference towards open access to government records in the U.S. contributes substantially to the economic well being of the nation (e.g. Pluijmers and Weiss 2002).

The FOIA of the national government as well as the open access laws of the individual states support generally a policy of broad disclosure by government. By example, if a data set held by a federal agency is determined to be an agency record, the record must be disclosed to any person requesting it unless the record falls within one of nine narrowly
drawn exemptions contained in the FOIA. Exemptions are construed narrowly by the courts so that disclosure is typically favored over non-disclosure.

Federal agencies also bear affirmative obligations to actively disseminate their information as defined by the provisions of Office of Management and Budget (OMB) Circular A-130 of June 1993 and the Paperwork Reduction Act of 1995 (PRA). As a result, federal agencies have been placing their digital geographic information openly on the web to make their data sets more accessible to other government agencies, for-profit businesses, non-profit organizations, and citizens generally (for example, see http://www.fgdc.gov/clearinghouse.html).

Exemption 1 under the U.S Freedom of Information Act states that the provisions of the act and thus mandates to release public records do not apply to matters that are "(1)(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order." Other FOIA exemptions that may justify the withholding by government agencies of geographic information in certain instances include data or records that are specifically exempted from disclosure by a federal statute (exemption 3) or records or information compiled by law enforcement agencies (exemption 7).

The extent and conditions under which material may be withheld by government under the FOIA exemptions and in the context of other regulations such as OMB Circular A-130 and the paperwork Reduction Act has been litigated extensively. Thus the case law and administrative rulings provide at least some guidance on whether or not a specific withholding by a federal government agency is allowable.

In withholding or withdrawing geographic data and related records, agency personnel should be able to cite the explicit statutory and administrative provisions authorizing them to do so. In the vast majority of instances we assume that the withholdings being made are in conformance with the law. However, even if specific withholdings are adjudged legal, questions now are being raised whether a general climate of increased government withholding of geographic data will increase or decrease homeland security and personal information privacy.

Effect of Access Policies on Security

The extent to which libraries and government agencies at federal, state, and local levels removed and are continuing to remove material in the interest of homeland security is difficult to determine. These actions typically are pursued internally with little fanfare. Much of the decision making at various government levels to remove specific materials appears to be rather ad hoc without serious consideration of the harms to other social objectives that such removals may cause. The question to be addressed here is not whether some or all of such removals are legal but whether such removals actually support the goals intended by their removal.

An example electronic document that depository libraries were requested to destroy was cited in the introduction. Even the title of this document suggests that it would supply a ready-made "hit list" for terrorists intent on infecting or otherwise disrupting the nation's water supply. While we no longer have access to the content of this document, the content may indeed have been of great interest to potential terrorists. However, questions remain regarding whether the information in the document would have been of even
greater value to those responding to terrorist acts and to the general public? It would take little investigation for a motivated terrorist to identify one or more major urban water supply aquifers in the U.S. If a terrorist incident were to occur, does the no longer accessible document supply valuable information that would be of great value to local emergency response teams and policy makers? Does it provide valuable information for local citizens and the news media who may want to verify for themselves that their specific water supply has or has not been affected by the incident? Would it be better that thousands of local citizens are aware of and watching the physical status and circumstances surrounding their own water supplies? Does the document provide valuable information for other important day-to-day beneficial decisions that will now be hampered?

In the World Trade Center case, locating this physical and political target took little effort on the part of terrorists. The target was obvious and no removal of mapping data would have altered the outcome. However, detailed maps and data were very much needed and relied upon by rescue and emergency personnel as well as by government officials and the news media. Because the Emergency Operation Center for New York City was destroyed in the twin towers collapse, the entire data center had to be reconstructed from scratch in order to supply needed emergency response maps and infrastructure information. The information system reconstruction effort was facilitated greatly by being able to access and copy data sets held at Hunter College as well as additional data sets held elsewhere in other public and private files (Cahan and Ball 2002). Had only one or a few copies existed, gaining access when needed would have been far more problematic.

One stream of logic for best providing homeland security in the U.S. relative to data access proceeds as follows:

1. The basic general policy assumption under U.S. law should continue to be "open access" to public records due to the huge social and economic benefits this policy supports.

2. It doesn't take detailed data or a sophisticated GIS for terrorists to locate prime targets. Such locations are readily available from innumerable sources. Legislatures and the public should also recognize that anyone can go to the web and within a couple of minutes type in a house address, produce a road map with detailed instructions on how to drive to the house, and print out an overhead satellite image that includes the house. These capabilities are used daily in this nation by vast numbers of people and the capabilities have many, many beneficial uses in society. The goal at the federal, state and local government level should be to achieve greatly expanded beneficial uses for our communities using similar GIS and spatial technology methods.

3. The best way to maintain the strongest national defense in the world is to maintain the strongest economy in the world. In an information economy, the proven way to accomplish this is to provide citizens and businesses with access to the raw materials (i.e. data, information and knowledge) they need to provide better information services and products to the nation and the world. Open nations will always have a distinct competitive advantage over those nations that don't provide broad citizen access to these raw materials. With a very strong economy, terrorists
and criminals can be dealt with. Criminals will always exist and we will always need to deal with them. Our past overall approach in the U.S. has been to let information systems (and technologies in general) rapidly evolve with few prospective controls in order to maximize economic stimulation and development. As a result, we have much greater leeway in this country to build on the works of others and experiment and play with data to provide new and better products and services to consumers. This has resulted in the strongest information industry and economy in the world. Our past perspective and the basis of our success has been to give great leeway to technologies to grow while passing laws that allow us to punish abusers of emerging technology. The presence of those who would abuse online systems should not deter us from making data available and useful to citizens in our communities who can reap many benefits from having more readily accessible government data. The benefits have far outweighed the drawbacks.

4. If information is power, we need to place it in the hands of every citizen so citizens can work together in myriad ways to solve the problems of society and improve the quality of their lives. Many repressive societies control their populations by allowing only a few elite to have access to maps and geographic information. Only a few nations have FOIA laws and none are as strong as those in the U.S. Open access to government information has been the tradition of our nation and the genius of our nation. It strongly supports the functioning of democracy and provides a huge economic multiplier effect. We need to expand that tradition in the information age, not retrench from it.

5. Improved information infrastructures and ready access to databases give us also the ability to track criminals much more effectively. It is difficult to operate in modern open societies without leaving digital tracks.

6. Democracy with strong civil liberties is the logical end-state of maximizing security (Dansby 2002). Although different from many other nations, citizens in the U.S. generally agree that suppression of free speech results in more damage than the effects of speech, no matter how offensive that speech may be. Similarly, general suppression of information of potential use to potential terrorists will often result in more damage to the nation than allowing the information to be accessible by all. With strong civil liberties and transparent government we are far more able to weather political, social, and economic disruptions over time.

Counter logic to the reasoning listed above as well as limits on the above statements obviously exist. Regardless, the above reasoning should at least be considered along with the more obvious counter arguments when considering whether to restrict access to a specific data set in the name of protecting national security or in formulating new government access policies.

Summary

"People don't quibble with the need for free speech. It is a liberty that people have defended with their lives. Freedom is always something you have to defend with your
life. But it's also not an easy choice to make initially. And the same is true of openness. You just have to make the choice to be open. It's a difficult stance to take at first, but it actually creates more stability in the end." (Torvalds 2001)

References


Dansby, Bishop, Personal correspondence, 2002


Torvalds, Linus and David Diamond, Just for Fun: The Story of an Accidental Revolutionary, Harper Business, p. 229