Freedom of Information or Right to Terrorize?

Limiting the Risks of Government-Mandated Information

by Angela Logomasini

Director of Risk and Environmental Policy
Competitive Enterprise Institute.

Presented at the Association of Private Enterprise Education
International Convention
Nassau, Bahamas
April 4-6, 2004

Introduction

Freedom of information has traditionally meant provision of government-generated information to the public for the purpose of holding government accountable for its actions. But in recent decades, "citizen" and environmental activists have worked to extend freedom of information to increased access to private information. To that end, they have advocated so-called "right to know" laws, which mandate that private firms generate information for the government to make public. They claim that access to such private information is analogous to freedom of information, even thought it involves government coercion to collect.

As a result, the government has been collecting and releasing massive amounts of private data, some of which might provide some value, but much of which is misleading or completely incomprehensible to the average person. In addition to being expensive for private firms to collect, government agencies spend considerable sums to post the data. The release of some of this information—particularly that which relates to the nation's utilities, chemical plants, and other critical infrastructure—has raised security concerns because it could assist terrorists in selecting targets and launching attacks. The security issue rose in prominence after September 11, 2001. As a result, policy makers have begun to limit public access to both government-generated data and privately generated data collected by government. While there are sure to be mistakes, and while we cannot control all data, there is good reason to control government provision of particularly sensitive information that could assist terrorists in attacking the nation's critical infrastructure. Such policies require that policymakers balance security concerns with the desire to provide data to the public.

Left-leaning "public interest groups" have suggested that any limitation on "right to know" information is unacceptable and somehow impedes freedom of information. They have even implied that such limits are a violation of the First Amendment, even though the amendment was designed to protect speech—not guarantee access to government collection and distribution of private information.[1] According to OMB Watch, government protection of information that public

[1] For example, the Society of Environmental Journalists, which publicly opposed the provision, includes "right-to-know" within the category of First Amendment issues, http://www.sej.org/foia/dhs_cii061603.

officials deem "sensitive" for security reasons sets a dangerous precedent in which the federal government and businesses could hide anything from the public.[2]

OMB Watch's view amounts to an overreaction that fails to acknowledge the fact that freedom of information policy has always included caveats. In addition to protecting officially classified data, the Freedom of Information Act (FOIA) provides exemptions for several categories of sensitive information, including: agencies' internal personnel rules and practices; information specifically exempted by other statutes; privileged interagency or intra-agency memoranda or letters; personal information affecting an individual's privacy; and investigatory records compiled for law enforcement purposes.[3] September 11 simply highlighted the need to consider national security concerns.

While exemptions are a necessary part of the law, access to a large portion of government information will remain an important part of keeping government accountable. It is reasonable to assume that data used to impact public policy, particularly government-funded research, should be publicly available as long as individuals involved in studies remain anonymous. Ironically, the groups opposing any reasonable limits to coercively collected private data are critical of the Federal Data Access Law and the Federal Data Quality Act, both of which are designed to provide public access to taxpayer-funded data that is used to influence and support federal regulations.[4] In contrast, rather than holding government accountable, "right-to-know" mandates are mostly designed to use private data to bolster government regulation, which appears to be the real agenda behind many of these laws.

Case Study: Clean Air Act Risk Management Plans

A provision buried in the 1990 amendments to the Clean Air Act requires facilities to develop risk management plans (RMPs), which are supposed to help them prepare for accidental

[2] OMB Watch, "Administration Gains New Power to Withhold 'Sensitive' Information," *Executive Report*, September 10, 2003, http://www.ombwatch.org/article/articleview/1799/1/39/
[3] 5 U.S.C. 552(b)
[4] For example see, OMB Watch, "Analysis of State Level Data Quality and Access Legislation," March 24, 2003, http://www.ombwatch.org/article/articleview/1393.

chemical releases. The law then directs the Environmental Protection Agency (EPA) to make these plans publicly available.

In its RMP, each facility must identify the chemicals it uses, state what quantities it stores on site, and detail mitigation measures it employs to control potential releases. The most controversial part of RMPs is the section on "offsite consequence analysis" (OCA), which includes a hypothetical "worst case scenario." For the worse case scenario, facilities describe what they think would happen in the event of a catastrophic chemical release by detailing, the potentially exposed population; the distance a release could travel under specified wind conditions; whether schools, daycare centers, and other receptors are located nearby; and related information. Security officials warn that this information could assist terrorists in launching attacks. In fact, RMPs provide *six out of nine* pieces of information that the Department of Defense lists as critical in launching a successful terrorist attack on an industrial facility.[5]

When the deadline for plants to submit RMPs drew to a close in 1998, EPA indicated its intent to post the plans on the Internet. But security experts—the FBI, CIA, International Association of Fire Chiefs (IAFC), and various other groups—raised alarm.[6] They feared that Internet posting would give terrorists easy, anonymous access to a searchable database of potential targets. In particular, OCA data would enable terrorists to rank facilities according to potentially exposed populations.

Congress revised the law in 1999, passing what security expert Amy E. Smithson of the Henry L. Stimson Center aptly calls "a dismally shortsighted compromise."[7] This law requested that DOJ and EPA issue a rule governing the process for releasing data in a way that minimizes security risks. Unfortunately, the agencies promulgated a rule that made the information readily available to nearly anyone.

---

[5] U.S. Department of Justice, Criminal Division, *Department of Justice Assessment of the Increased Risk of Terrorism or Other Criminal Activity Associated with the Posting of Off-Site Consequence Analysis Information on the Internet*, April 18, 2000, p. 2, http://www.usdoj.gov/criminal/april18final.pdf.

[6] For more discussion on this debate, see Angela Logomasini, "The Clean Air Act's Terrorist Assistance Program," *CEI On Point*, May 21, 1999.

[7] Statement of Amy E. Smithson, Ph.D., Director of Chemical and Biological Weapons Nonproliferation Project, Henry L. Stimson Center, Before the House Committee on Transportation and Infrastructure, Subcommittee on Water Resources and Environment, November 8, 2001.

The new law did include one key reform: It provided EPA with a FOIA exemption that prevented environmental groups from accessing the full information in electronic format (which would allow easy posting on the Internet). Yet this reform mattered little given that EPA opted to post the bulk of the information on the Internet in 2000—including about 50 percent of the "worst-case scenario" sections as well as full executive summaries.

The reformed law also mandated that EPA make the entire plans available in 50 federal "reading rooms" throughout the nation, which the agency did starting in January 2001. Individuals merely need to show an identification card to view all the details and take notes on up to 10 facilities per month. Furthermore, the law does not bar anyone from collecting and posting all of this information online.

After the new law passed and while EPA was posting the data online, the Department of Justice (DOJ) released a report regarding security risks associated with the data. According to DOJ, the types of facilities that submit data to EPA are "preferred targets" for terrorists, such as plants located in high-population areas, military installations, and infrastructure. Fifteen percent fall into the category of basic infrastructure: about 2,000 are water supply and irrigation facilities; 80 are military installations; 56 are related to electricity supply, transmission, and control; and 14 involve natural gas distribution. "Disruption of even one of these facilities could wreak havoc on an entire region or locality," said DOJ in 2000.[8]

After September 11, public officials finally pulled the RMPs and their summaries off federal Internet sites. Yet the federal government still makes the full information easily accessible at federal libraries.[9]

Unfortunately, OMB Watch had already downloaded the summaries from EPA's website, and it continues to host them online today.[10] Some summaries include OCA data, but the amount and quality of information they offer varies widely from one summary to the next. Some

[8] U. S. Department of Justice, *Department of Justice Assessment*, p. 20.
[9] The author scheduled an appointment at EPA to view the full RMPs, and viewed them February 7, 2002. After simply showing my driver's license and signing a sheet of paper, the author collected data on 10 facilities in less than an hour. Facilities were selected facilities before going to the library by searching the executive summaries online.
[10] OMB Watch hosts the summaries on a page called The Right to Know Network, http://www.rtk.net.

summaries are nearly as detailed as the plans themselves and some include additional details. Many summaries feature figures related to potentially exposed populations.

OMB Watch and the Center for Public Data Access host the website called "Right to Know Network," which allows for searching of 15,000 RMP summaries, making targeted searches of sensitive information very easy. For example, a search of the terms "school and child care" brings up numerous summaries. One notes a that release could reach "fifteen school and daycare facilities, one hospital …" A follow-up trip to the library[11] reveals that the release would involve 2,000 pounds of chlorine gas that, traveling at a wind speed of 1.3 miles per hour, could reach 10,000 people.

In addition, the summaries can be very detailed, providing information that means little to the average person, but that could assist in the planning of an attack by providing information on optimal conditions to cause maximum fatalities and injuries. A couple of examples include:

> "For worst case, it is assumed that the EO [Ethylene Oxide] is released into the atmosphere in a ten minute time period. EPA's Degadis computer model was used to model the toxic endpoint. Assumptions in the model are: 1) Wind Speed = 1.5 m/s; 2) Stability Class = F; 3) Air Temperature = 77 degrees Fahrenheit. Using the model, the toxic endpoint was estimated to occur at a distance of 4,500 meters (2.80 miles) from the center of the facility. Estimated population in that radius is 124,345 people."

> "The Worst Case Release Scenario at … was defined by the following conditions: Failure of the single container resulting in the total release of 21,500 pounds of anhydrous ammonia; Release of the entire amount as a gas in 10 minutes; Use of the one-hour average ERPG-2 as the toxic endpoint; Consideration of the population residing within a full circle with radius corresponding to the toxic endpoint distance; and EPA mandated meteorological conditions, specifically an F atmospheric stability class, wind speed of 1.5 m/sec, and air temperature of 771F. Atmospheric dispersion modeling for the Worst Case Release scenario resulted in a ammonia endpoint distance of 1.5 miles and an estimated residential population potentially affected of 8,747."

In addition, the news industry also helps those who want to select targets by highlighting which facilities would cause the greatest damage if attacked.

Environmental and "citizen" activists claim this information is valuable because they say it informs the public about risks in their communities. In reality, it does nothing of the sort. RMPs include fictitious scenarios of the most highly unlikely catastrophic chemical releases. Accidents

[11] The author visited the EPA RMP reading room on February 7, 2002.

may happen in the real world, but these scenarios go well beyond the realm of reality. They assume that every mitigation measure at a plant would fail and that nothing would be done to control a release. Nor do the plans provide the type of information that could save lives should an accidental release occur: RMPs don't educate the public on how to respond in the event of an emergency.

There is a reason why the Clean Air Act demands that RMPs be drafted in this manner. Those who wrote the provision designed it to serve a radical environmental agenda, one that focuses on elimination of chemicals. If activists can use this information to scare the public, they can mobilize them to push for greater regulation and eventual bans.

In fact, three months after EPA made RMPs available in public libraries, Greenpeace published horror stories on the Internet: "Greenpeace and the Working Group on CRTK [community right to know] collected this alarming data from the U.S. EPA reading room in Washington, D.C.," the organization's press release read. "The data released today is for companies reporting worst case scenarios that could put 100,000 or more people at risk," it continued. Along with the press release, Greenpeace posted numerous maps of potential releases, which include the location of schools, hospitals, and population figures. The activist group even listed 50 facilities along with population data, enabling terrorists to rank those plants according to the size of populations at risk—exactly what security experts wanted to avoid.[12]

After September 11, security officials highlighted further the dangers of keeping this information easily accessible. "The information [about worst-case scenarios] is important to local emergency responders, but we are not for putting it out there for anyone to use … online or in reading rooms," says John Eversole, retired fire chief for the Chicago Fire Department and current chair of the Hazardous Materials Committee of the IAFC. Chances are too high that someone will use it to attack the nation's infrastructure, Eversole contends.[13]

Eversole does not oppose providing reasonable information to the public. He says that fire chiefs should be the ones to communicate with individuals regarding risks. Fire chiefs, says

[12] Greenpeace USA, "Bhopal In The Bayou, Are Chemical Accidents A Trade Secret?: Environmental Groups Release Unpublished Accident Scenario Reports," March 22, 2001, http://www.greenpeaceusa.org/media.
[13] Telephone conversation with Mr. Eversole, February 19, 2002.

Eversole, will provide better information, including what to do in the case of an emergency. "But we are not going to tell you specifics such as what is there, in what tanks, or how one could create an accident," he says. The IAFC has opposed the distribution of that information, but since September 11, fire chiefs are "doubly" concerned about the availability of RMPs, says Eversole.

Security expert Amy Smithson called the release of RMPs a "terribly ill-advised regulation" during a congressional hearing. She and her colleagues conducted interviews with emergency first responders in 33 cities within 25 states during 1999 and 2000. According to Smithson, these responders echoed her concerns about the release of this information.[14] The public agrees with security officials on this issue. A recent poll conducted by the Pew Internet & American Life Project found that 69 percent of those polled believe the government should do whatever is necessary to keep such information out of the hands of terrorists—even if that deprives the public of information it wants.[15]

A better balance would be achieved by having emergency responders serve as the source of public information on potential risks. They can inform communities on how to respond in the case of an emergency, as John Eversole of the IAFC recommends. Plans should be removed from libraries and private groups that host summaries on their websites could be encouraged to remove them voluntarily. This approach would serve communities better by giving them valuable information, rather than inundating them with fictitious horror stories.

Post-9/11 Congressional and Administration Actions

After 9/11, Congress finally began to recognize the importance of considering security concerns before releasing private information collected by government. In 2002, Congress passed the Public Health Security and Bioterrorism Preparedness and Responsiveness Act of 2002, which included a provision requiring drinking water facilities to produce "vulnerability assessments" that outline risks associated with possible terrorist events. Congress exercised

[14] Statement of Amy E. Smithson Before the House Committee on Transportation and Infrastructure.

[15] Pew Internet and American Live Project, *One year later: September 11 and the Internet, September 5, 2002,* http://www.pewinternet.org/reports/pdfs/PIP_9-11_Report.pdf.

some wisdom regarding distribution of this information, providing that the information be approved by EPA but not released to the public.[16] However, these vulnerability assessments are still potentially available under state and local sunshine laws. Many states have begun to address this issue, but the Association of Metropolitan Water Agencies warned last September that many states had not yet passed measures necessary to "protect sensitive information that could be used to disrupt or destroy drinking water systems."[17]

In addition, the Homeland Security Act included another security exemption to FOIA. It limits agency release of information that private parties voluntarily provide to agencies for the purposes of assisting in homeland security efforts. The provision reads:

> "Notwithstanding any other provision of law, critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement."[18]

The goal behind this provision is to encourage information sharing by eliminating fears that critical information about the nation's infrastructure would become public. The debate over this provision was contentious, with OMB Watch, the American Civil Liberties Union, journalists, and environmental groups claiming that it could enable firms to label anything confidential.[19]

Opposition continues as the law is being challenged by legislation offered by Senator Patrick Leahy (D-Vt), (whose amendment to change this provision lost in a floor vote when the Homeland Security bill was considered in the Senate) to partially reverse this provision. Leahy claims that the Homeland Security Act "effectively allows companies to hide information about

---

[16] 42 USC §300i-2.

[17] "Majority of States Amending Disclosure Laws To Protect Security-Related Information," *Daily Environment Report*, September25, 2003, A-6.

[18] Pub. L. No. 107-296, 116 Stat. 2135, § 214(a)(1)(A); To be codified at 6 U.S.C. § 133(a)(1)(A).

[19] OMB Watch, "All Aboard the Homeland Security Express Bill Creates Dangerous New FOIA Exemption," November 20, 2002, http://www.ombwatch.org/article/articleview/1194; see also: Coalition Letter to Congress Urging Opposition to the Broad Freedom of Information Act Exemption in the Homeland Security Act, posted on the American Civil Liberties Union Website at: http://www.aclu.org/NationalSecurity/NationalSecurity.cfm?ID=10525&c=111

public health and safety from American citizens simply by submitting it to [the Department of Homeland Security]."[20]

However, the law provides exemptions for private firms and local governments that provide information on a *voluntary* basis. It does *not* prevent the release of government-generated, federally mandated, or taxpayer-funded information. And without the law, firms could still "hide" this information by simply choosing not to provide the government any extra information. But that wouldn't serve the public since it would make security planning more difficult.

Moreover, this new provision doesn't actually change existing law very much, but instead will help enforce it. Even before the passage of the Homeland Security Act, FOIA preempted the release of this information. A federal court ruled in 1992 that federal agencies are not supposed to release data that is: 1) voluntarily provided to agencies; 2) is commercial in nature; and 3) is not the type of information usually released to the public. Yet many agencies have failed to comply with this case.[21] The new law will simply ensure compliance.

Despite the fact that OMB Watch and others suggest that this provision will enable firms to keep anything confidential, others believe that it still can't provide enough privacy for sensitive data. Private firms and public utilities are still fearful to provide information because they are concerned about potential government security lapses and loopholes under which the information might still be released. The General Accounting Office (GAO) reported in 2003, that information-sharing necessary to protect critical infrastructure is being inhibited because industries fear that their sensitive and private data will be released under FOIA—even given the protections provided under the Homeland Security Act. In 1998, President Clinton released Presidential Directive 63 to encourage industries to form information-sharing associations called Information Sharing Analysis Centers, which are designed to collect and provide information necessary to protect the

[20] Juliana Gruenwald, Meredith Preston, and Patricia Ware, "Senators Introduce Legislation to Limit FOIA Exemption in Homeland Security Law," *Daily Environment Report*, March 13, 2003, A-8.
[21] *Critical Mass Energy Project v. NRC*, 975 F. 2nd 871 (DC Cir 1992). For a discussion see: Gerald H. Yamada, "Federal Agency Policies Imperil Privacy of Business Information," *Legal Opinion Letter* 12, no. 8, (Washington, D.C.: Washington Legal Foundation, April 5, 2002).

nation's critical infrastructure. GAO reports that a review of five such centers shows that all five have cited FOIA as a serious impediment to provision of emergency planning information.[22]

There is good reason for concern. Not only have agencies ignored FOIA exemptions in the past, there have been serious security mistakes. EPA has received repeated warnings from its own inspector general as well as from Congress that private data on its Internet site was not secure. In 1997, the EPA Office of Inspector General reported that they had discovered several instances in which outside parties hacked into EPA databases containing confidential information. The inspector general report concluded: "Although there are six documented hacker attacks on EPA systems, it is likely the number of actual attacks is much greater."[23] In 1999, the agency admitted that it lost about 500 confidential records that companies filed with the agency under the Toxics Substances Control Act.[24] In February 2000, EPA had to temporarily shut down its entire site after GAO workers were able to hack into the agency's allegedly secure pages.[25] And in 2002, EPA's Inspector General reported that the agency had unintentionally posted online portions of the off-site consequence analysis data that was not authorized for release online. The data were available for download between April and June 2001.[26]

Conclusions

Freedom of Information should remain an important part of providing oversight to the activities of government. However, "citizen" activist groups have wrongly equated freedom of information with "right-to-know" laws that compel private entities to assemble and submit data to the government, which then makes it widely available to the public. By overlooking serious

---

[22] U.S. General Accounting Office, *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors*, GAO-03-233 (Washington, D.C.: USGAO, February 2003), http://www.gao.gov/new.items/d03233.pdf.

[23] Charles Bogino, "Agency Cuts Access to Internet Material, Citing Need to Improve Computer Security," *Daily Environment Report*, February 18, 2000, AA-1.

[24] Sara Thurin Rollin, "EPA Notifying 190 Chemical Companies About Losing 500 Confidential Records," *Daily Environment Report*, December 23, 1999, AA-1.

[25] Ibid.; U.S. General Accounting Office, *Information Security: Fundamental Weakness Place EPA Data and Operations at Risk* (Washington, D.C.: U.S. General Accounting Office, July 2000).

[26] EPA Office of the Inspector General, Information Technology: Review of Offsite Consequence Analysis Information and Management, Audit Report 2002-P-0006 (Washington, D.C.: U.S. Environmental Protection Agency, March 22, 2002), http://www.epa.gov/oigearth/reports/2001/AuditRpt_2002_P_00006.pdf.

problems with such wide distribution of some of the data, the federal government has created unnecessary security risks for the public. While September 11, 2001 served as a wakeup call for regulators and politicians regarding distribution of this information, problems remain as agencies continued to be pressured by groups claiming the right to private data.