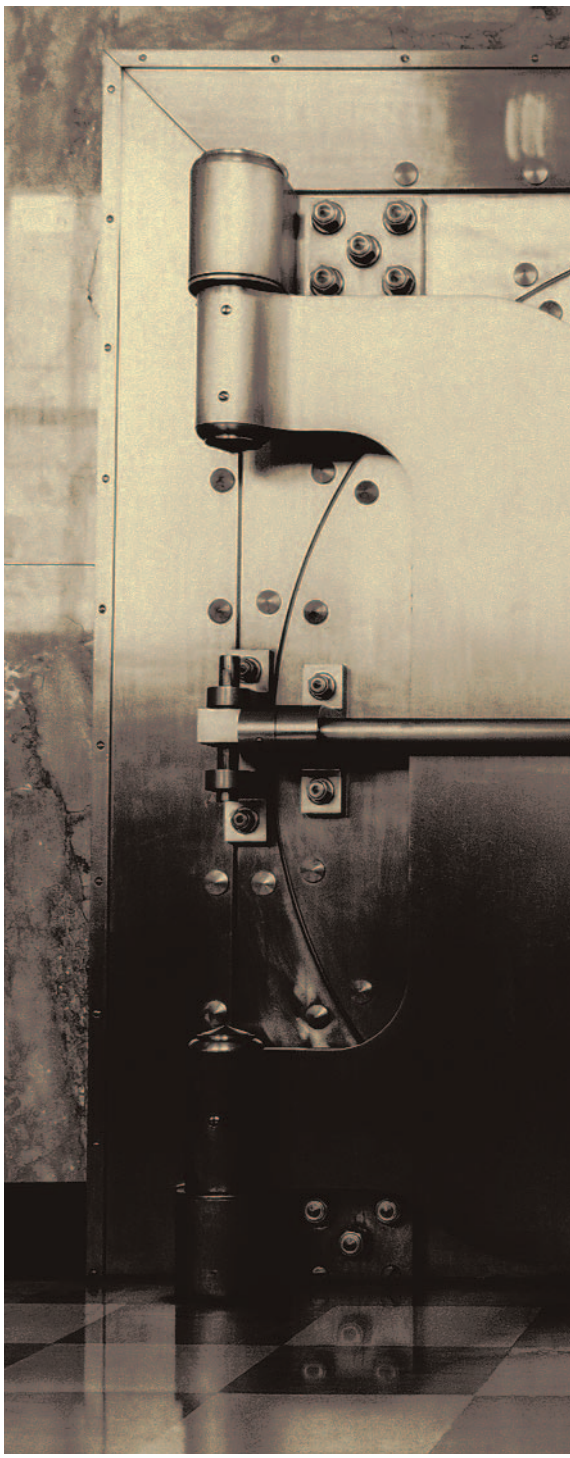
Does Secrecy Equal Security?

Limiting Access to Environmental Information



Digital Vision

After the terrorist attacks of 11 September 2001, the response by governmental agencies frightened by the prospect of more terrorist action was swift. Agencies that routinely provided information about the environment, public health, and physical infrastructure on their websites removed those resources in the belief that terrorists might learn where the nation is most vulnerable merely by surfing the Internet.

While some of the information has been restored to websites, much remains unavailable. And not only is there less governmental information on the Internet, but the threat of terrorism also has strengthened a pre-existing movement to place greater restrictions on public access to information that industry and government once had been required to make available. Some critics of such policies are wondering whether secrecy actually equals security.

Once, a Philosophy of Openness

Even before the terrorist attacks of September 11, the issue of public access to sensitive environmental information was the subject of often heated debate. But since the passage of the Freedom of Information Act (FOIA) in 1966, federal officials have been required to have very good reasons for keeping data secret because, legislators reasoned, the public has a right to know what the government is doing. FOIA created a new era of governmental transparency, and further resulted in new laws and regulations requiring that industry be likewise forthcoming with the public.

When Congress amended the Clean Air Act in 1990, this philosophy of openness took a new form. Section 112(r) of the act required that industrial facilities create "risk management plans" (RMPs) that detail what their operators are doing to prevent chemical releases and what they would do if chemical accidents occurred. They were also required to submit summaries of the RMPs to the U.S. Environmental Protection Agency (EPA) by 1999. By law, this information is available to the public.

Many companies fought this requirement; among other reasons—including that it might reveal trade secrets—they claimed that this kind of information could be dangerous if it fell into the hands of terrorists. When the EPA indicated that it wanted to post the information on the Internet, opponents spoke out and cited, among their arguments, the contention that the information might help terrorists locate potential targets.

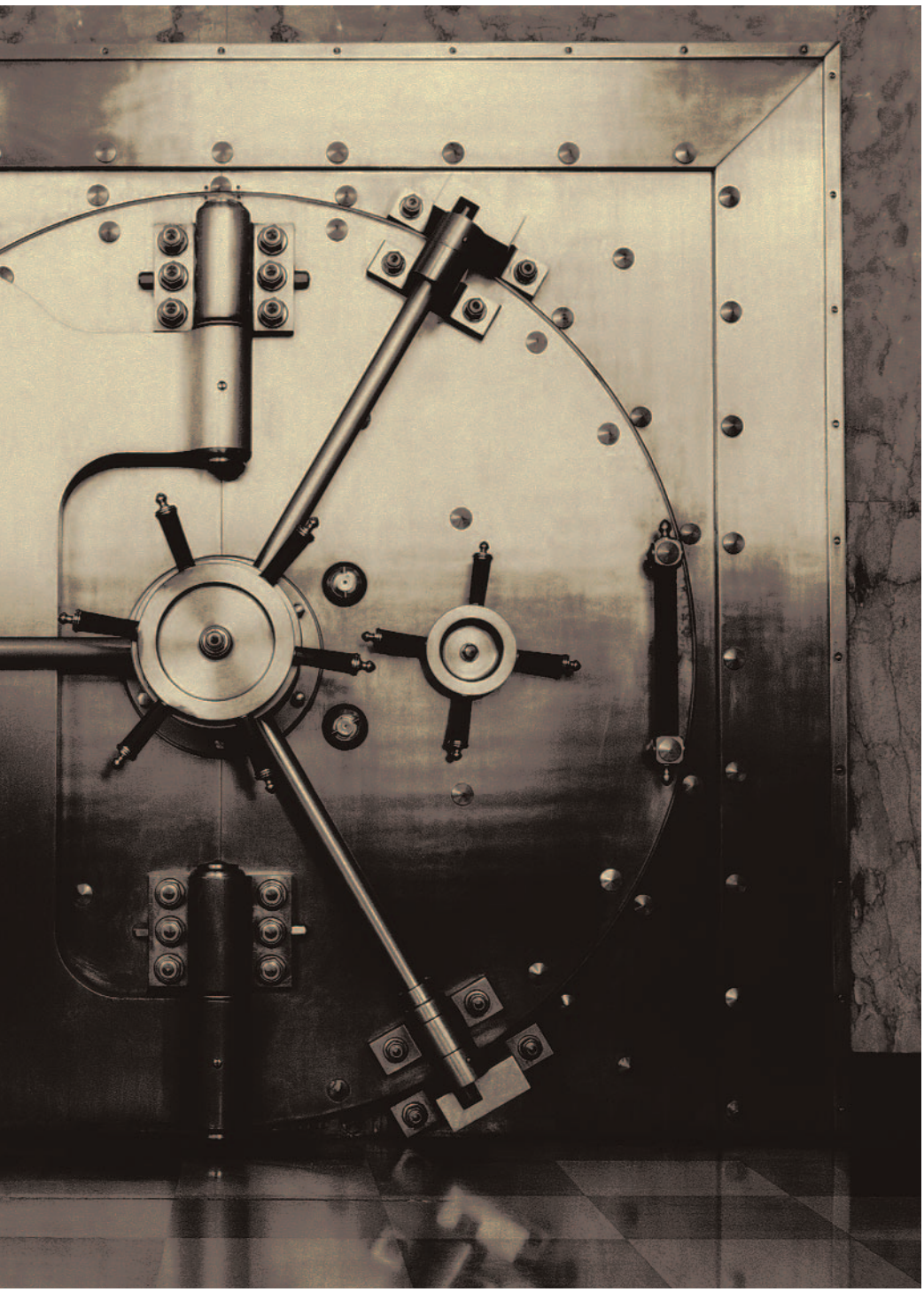
In 1998, as the deadline for plan submission drew close, the EPA agreed to keep certain RMP sections off the Internet. Congress stepped in and told the EPA and the Department of Justice to develop a joint rule that would reduce security risks while still making the information available to the public. The two entities responded with a joint rule that left most of the information on the Internet but diverted the most sensitive information—a section in the RMPs called the "offsite consequence analysis" (OCA), which describes potential impacts to the community resulting from worst-case scenarios involving chemical releases—to 50 secure reading rooms around the country.

Visitors to these reading rooms, which are located in each of the EPA's 10 regional offices and other federal buildings, must have government-issued identification, and cameras are forbidden. The libraries also track who has requested documents and which specific documents they viewed. In addition, no one can see more than 10 documents per month.

Elaine Stanley, the recently retired director of the EPA Office of Information Analysis and Access, says the chief concern regarding the OCAs is that their purpose is to show how the submitting company would deal with worst-case scenarios, including the potential impact of a chemical release. "Yes, the RMPs show the existence of and storage of quantities of chemicals, but frankly that information is available in a variety of different databases," she says. The OCAs, on the other hand, particularly with the scenarios and degree of detail that they contain, offer terrorists an open book on how to deliver the greatest blow to a community.

New Fears, New Restrictions

That was the situation when terrorists struck on September 11. Like many agencies, the EPA quickly responded by removing potentially risky information—including the RMP database—from its website. According to Stanley, most of the information was restored to the website within a day or two—except the RMPs, which today remain unavailable from the EPA website. The full RMPs, including the OCAs, are available in limited quantities for reading only to anyone who wants to travel to one of the reading rooms. People can also obtain copies of the plans



from the EPA through a FOIA request, but they will lack the OCAs.

In addition to the EPA's removal of the RMP information, the Department of Transportation has taken down all its information about pipeline routes, the National Geospatial-Intelligence Agency (formerly the National Imagery and Mapping Agency) has stopped selling large-scale digital maps, and the Government Printing Office sent out a directive ordering all government libraries to destroy copies of a CD-ROM describing public water supplies. The Nuclear Regulatory Commission shut down its entire website. The Agency for Toxic Substances and Disease Registry removed a report, *Industrial Chemicals and Terrorism: Human Health Threat Analysis, Mitigation and Prevention*, which was critical of security at chemical plants in general (but which did not provide specific information on specific facilities). And the Federal Energy Regulatory Commission removed thousands of online documents that gave information about hydropower plants, natural gas and oil pipelines, electric transmission lines, and other infrastructure.

For the first six months or so after September 11, agencies were on their own as far as what they decided to remove. Then, in March 2002, White House Chief of Staff Andrew Card distributed a memo, accompanied by a memo from the Department of Justice, calling for creation of a new "sensitive but unclassified" designation for information and urging agencies to be more careful in what they made available to the public. Shortly thereafter, the "sensitive but unclassified" language appeared in the Homeland Security Act. The Defense Department has reportedly removed 6,000 online documents in response to the Card memo.

But according to OMB Watch, a nonprofit group that promotes governmental accountability and citizen participation in public policy decision making, the Homeland Security language about the "sensitive but unclassified" category is vague; of this category, the Homeland Security Act states, "The needs of State and local personnel to have access to relevant homeland security information to combat terrorism must be reconciled with the need to preserve the protected status of such information and to protect the sources and methods used to acquire such information."

"What the heck is 'sensitive but unclassified' information?" asks Rick Blum, director of the Freedom of Information Project at OMB Watch. "The definition that's provided in the statute is so broad, our concern is that [it] could really inhibit discussions about protecting human health and the environment." According to OMB Watch, there is no firm, overarching government policy on what kinds of information to restrict, and restrictions are often placed by lower-level staff acting on their own.

The Battle for Access

Even though the EPA removed the RMPs from their website, some environmental groups had already downloaded the information and continue to make it available online today. Angela Logomasini, director of risk and environmental policy at the conservative Competitive Enterprise Institute, a critic of policies providing easy access to potentially sensitive environmental information, believes there's not much Congress can do about private groups providing the information on the Internet. But she doesn't think Congress should make it easy for such groups to make this information so readily available, especially the information about worst-case scenarios.

"The question is, how useful is this information to the public?" she says. "If a person in a community wants to know what the risks are, scaring them with these worst-case scenarios is probably less valuable than letting them know what to do if there is a release. The RMPs don't provide that kind of information."

Stephen Dycus, a professor at the Vermont Law School and an authority on national security and the law, who has been monitoring the growth of government secrecy since the terrorist attacks, notes there is a law that does provide that kind of information: the Emergency Planning and Community Right to Know Act, which requires that facilities compile toxic release inventories of the chemicals that are present and make that information available to first responders (for example, firefighters and police). There's also a public right to know provision, requiring that states create offices to handle that function.

Blum disagrees with the idea that information should be withheld from the public. "Openness can make you safer," he says. "When there's openness, there's accountability. And that can help us [identify system vulnerabilities] before the terrorists do. We want openness so the public can hold government officials and companies accountable."

Blum contends that the safer havens provided by such new creations as "sensitive but unclassified" may already be having an effect on public health. He points to roadblocks faced by a citizens group in Aberdeen, Maryland, that has filed suit against the U.S. Army under the Comprehensive Environmental Response, Compensation, and Liability Act (Superfund) over the growing presence of perchlorate in the aquifer that feeds the city's drinking water supply. The perchlorate, a chemical used in rocket fuel that is drawing increasing attention from scientists trying to determine its toxicity, is apparently originating from the Army's nearby Aberdeen Proving Ground.

Christopher Gozdor, a lawyer at the University of Maryland Center for Health and Homeland Security who represented the group last year while a student attorney with the University of Maryland Environmental Law Clinic, says that in the 1990s, the Army quickly responded to the presence of trichloroethane in the city's water supply by building a $2.2 million groundwater treatment plant. But when the perchlorate appeared last year, the Army's response was a stark change from its prior forthcoming relationship with the community: "It wasn't that the Army would completely withhold disclosure," he says. "Information was coming out, but it wasn't on the kinds of maps that are useful to environmental scientists so that they could track movement of plumes." The maps, he says, have been censored to the point that they are "almost devoid of detail"—street names, locations of buildings, concrete surfaces, and other features have all been removed.

Digital Vision, Photodisc, Chris Reuther/EHP

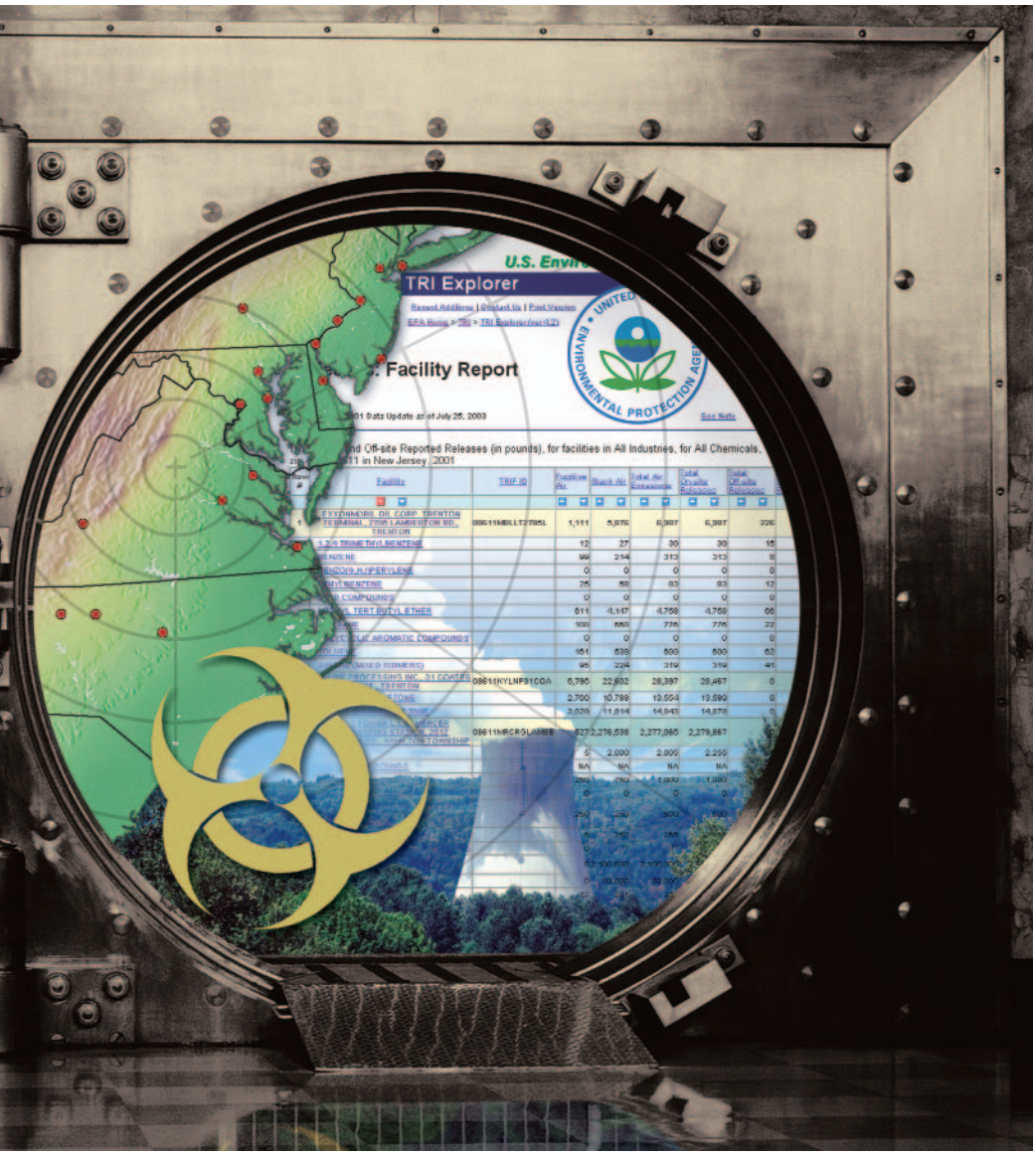
Rena Steinzor, director of the University of Maryland Environmental Law Clinic, now represents the citizens group. She filed suit against the Army in August because she says the Superfund law, which governs cleanup at federal facilities, contains disclosure requirements that are not being met. "Our basic point," she says, "is that we object to this kind of operating in the shadows for withholding information." And without the Army's cooperation, the citizens of Aberdeen don't really know how big the perchlorate problem is.

Growing Secrecy

Meanwhile, in May 2002 President George Bush signed an order giving the administrator of the EPA "original classification authority"—the power to stamp any EPA document as classified. "Why, exactly, the EPA administrator has been given that power is not entirely clear," says Dycus. "But it suggests that in the future we can expect some EPA documents that might have been available otherwise not to be."

But the authority is not intended to be used to classify any EPA document that is controversial or that may contain unpleasant revelations, says Jon Edwards, deputy director of the EPA Office of Homeland Security. Instead, the authority is granted to the administrator to classify EPA-generated documents that may have very sensitive national security information, such as research results on certain environmental aspects of weapons of mass destruction.

On 25 March 2003, Bush signed Executive Order 13292, which amended a 1995 order by former president Bill



Clinton, greatly strengthening government officials' powers to classify information. Examination of the two orders reveals how dramatically governmental attitude toward secrecy has changed under the Bush administration. The Clinton order contained a presumption in favor of disclosure—if in doubt, don't classify. The Bush order reverses the presumption, placing a greater burden on people who want information.

Dycus says that Executive Order 13292 adds two new classification categories—"transnational terrorism" and "vulnerabilities or capabilities" of infrastructures—to the secrecy list. That is, if claims can be made that information is related to defense against transnational terrorism or in need of secrecy to protect vulnerable infrastructure, it is classifiable. "[These categories] suggest the potential . . . to keep environmental information secret that might not otherwise be classifiable," he says.

Yet another example of a shift toward greater governmental secrecy is a new Critical Infrastructure Information rule written under the Homeland Security Act. This rule enables private companies to send information to the Department of Homeland Security, whereupon it is automatically exempted from disclosure under FOIA and cannot be used against the submitting company in a lawsuit. Blum notes, "The idea was that theoretically this would enable the government to learn more about where our weaknesses are and maybe do something about it." But the rule is not being tested before implementation—"there's no sunset," says Blum. "There's no thirty-day clock. It's an indefinite restriction on access." (The Department of Homeland Security was unresponsive to requests to comment upon this article.)

Sean Moulton, senior information policy analyst at OMB Watch, argues that government is going too far in trying to fight terrorism by reducing public access to environmental information. "The unfortunate situation is that the people making these policies are so shortsighted that they don't realize there's a safety cost involved in restricting this information," he says. "Very often, I hear people say, 'If restricting this information protects one person, then I say we should withdraw it.' What they don't seem to realize is that pulling the information down may actually wind up hurting someone or actually costing someone their life."

A Need for Balance

Although proponents of broad access to environmental information argue that a fully informed society is a better society, they do agree that the terrorist threat may require certain prudent limits on access. "I would not argue that some of the information that's being protected doesn't need to be protected," says Dycus. "What's tricky is finding the right balance between protection from terrorists on one hand and providing information for the neighbors so they can keep themselves safe. Throughout the Cold War, in the name of national security, the government didn't tell the neighbors squat about anything—and the results, we now know [as in the Love Canal case of the 1970s], were catastrophic. This is really no different."

"We need to find ways that we can nest the two together," says Moulton. "I think we need to figure out some criteria. If we're going to restrict some information, it needs to be a very precise decision. We need to figure out what's too dangerous and just restrict that. But right now, . . . government is using a sledgehammer."

Logomasini counters that "public right to know" might just as aptly be called "terrorists' right to know." She says a more sensible approach would be to restrict information on practical responses to local emergency responders such as fire chiefs, who might then communicate the risks to the community.

Dycus thinks that level of restriction is going too far. He believes that to a certain degree, certain politicians and their industry supporters are using the terrorism argument and their call for greater secrecy as a smoke screen to protect industry from lawsuits or bad publicity. "Those are not reasons for drawing curtains on this sort of information," he says. "I don't have any neat formulas for how to do this; it's largely a matter of common sense. What I am convinced of is that before information that concerns the public in such an intimate way should be kept from the public, the government needs to demonstrate a very compelling reason for keeping it secret."

Richard Dahl