Giving Away the Store: The Flaws in EPA's Expanded Right to Know Program

William H. Lash III

Contemporary Issues Series 92

August 1998

Center for the
Study of
American Business

Washington University in St. Louis

This booklet is one in a series to enhance the understanding of the private enterprise system and the key forces affecting it. The series provides a forum for considering vital current issues in public policy and for communicating these views to a wide audience in the business, government, and academic communities.

The Center for the Study of American Business is a nonprofit, nonpartisan organization funded entirely by grants from foundations, business firms, and private citizens. Funding is unrestricted, enabling researchers to maintain academic freedom and ensuring unbiased and independent research. The Center is an integral part of Washington University, which has been granted tax-exempt status under section 501(c)(3) of the Internal Revenue Code. Donations to the Center qualify as charitable deductions for income tax purposes.

Donations can be made to the Center at the following address:

Center for the Study of American Business
Washington University
Campus Box 1027
One Brookings Drive
St. Louis, MO 63130-4899

The opinions expressed are those of the author and not necessarily those of the Center for the Study of American Business or Washington University.

Giving Away the Store: The flaws in EPA's Expanded Right to Know Program

William H. Lash III

Introduction

One point on which most economists agree is that dissemination of information helps markets operate more efficiently. Improved access to information allows people to make better decisions and evaluate risks more easily. However, all information should not be widely disseminated as prices of canned goods at the supermarket or stock prices on the floor of the New York Stock Exchange. The old question, "Does Macy's tell Gimbel's?" notes the importance of keeping some information secret from competitors. Similarly, information which might impact national security needs to be safeguarded.

These well-accepted reasons for preserving confidential business information are under attack by the Environmental Protection Agency (EPA) and environmental activists. EPA plans to disclose an unprecedented amount of manufacturing secrets from more than 66,000 firms via the Internet. Once on line, crucial information will be available to not only concerned citizens but also foreign competitors and even terrorists.

This paper will discuss the EPA's expanded "right to know" program and the threats it may pose for American firms and public safety.

William H. Lash III is a Distinguished Senior Fellow of the Center for the Study of American Business at Washington University in St. Louis and a professor of law at the George Mason University School of Law.

Right to Know and the Risk of Terrorism

The Clean Air Act amendments of 1990 mandated that "risk management plans" (RMP) be written for more than 66,000 industrial facilities, including chemical plants, oil and gas refineries, pharmaceutical companies, electric and gas utilities, and waste water treatment works. Military and energy facilities of the federal government also are required to establish risk management plans. The plans must include evaluations of the risks and hazards at each installation, as well as discuss accident prevention and proposed responses to an accidental release for nearly 200 hazardous substances. Each firm also must develop an "offsite consequence analysis" (OCA). The OCA for each facility must analyze the dangers to the public and the environment by possible accidental releases.

The most controversial part of these requirements is the preparation of "worst case scenarios." A worst case scenario must disclose: (1) the chemical or hazardous material that might cause the worst case scenario if released, (2) its physical state, i.e., gas or liquid, (3) the amount of the material that would need to be released to cause the situation.

These evaluations also must identify possible causes of a release leading to the worst case scenario. The topography of the area in which the plant is located and the reach and range of the effects of the release must be included. And the description must estimate the number of people injured, killed, or otherwise "affected" by the release.[1]

Firms also must disclose their addresses and locations by longitude and latitude, the nature and amounts of hazardous materials on site, and the number of full-time employees at the site.

The Clean Air Act specified the type of information to be disclosed, but did not state how the data was to be made available. EPA has decided to disseminate this information via the Internet. Though Internet access tremendously lowers information costs to the public, it simultaneously raises the threat of economic espionage and the dangerous

use of this information by terrorists.

Initially EPA planned to post OCA data freely on the Internet. The agency revised this decision after being made aware of the risks of disclosing this type of information. EPA now says that OCA data will be made subject to electronic controls, making it more difficult for terrorists to access.[2]

But the other data disclosed will still pose significant risks for firms. A study by Aegis Research Corporation, commissioned by the EPA, notes that ready access to chemical risk information concerning U.S. firms would offer terrorists "the capability to scan across the entire country for the 'best targets.'"[3]

EPA has decided to disseminate this information via the Internet....[which] raises the threat of economic espionage and the dangerous use of this information by terrorists.

Environmentalists have dismissed the threat of increased terrorism resulting from disclosure of Risk Management Plans. According to Fred Millar, a former director of the Toxics Project of Friends of the Earth, "It is necessary to inform the public in order to get an appropriate level of concern," prompting firms to "reduce their risks of accidents."[4] Mr. Millar, who helped draft the amended Clean Air Act, asserts that "there is no credible history of terrorist threats" targeting the chemical industry.[5]

Mr. Millar bases his prediction on an antiquated model of terrorism, a model predating the Internet. He also ignores the admonitions of security experts. By making the information more readily available, terrorists can receive targeting information free of charge from the safety of their own homes. Even advocates of disclosure acknowledge that posting the data on the Internet will "whet the appetites" of terrorists.[6]

The CIA and the FBI are opposed to EPA's

Internet disclosure plans. FBI spokesman Paul Bresson observed,

> They, the EPA, have to enact the law. But at the same time, can they use another mechanism, another vehicle besides the Internet?[7]

Similarly, Christopher Ronay, head of the Institute of Makers of Explosives and a former member of the FBI, said,

> I don't think we're in opposition to the public knowing these facilities are present…But I don't think we want to post on the Internet...the facility's (locale) and exactly what's in it.[8]

The Chemical Manufacturers Association (CMA) supported the Clean Air Act amendments in 1990 and public disclosure of worst case scenario data. Its president, Fred Webber, affirms CMA's continued support for the plan to make the data publicly available. The association, however, is opposed to disclosure of Risk Management Plan data via the Internet.[9]

Congressional leaders have joined the FBI and the business community in expressing concern about the disclosure plans. In a letter to EPA administrator Carol Browner, Senate Majority Leader Trent Lott warned that the Internet disclosure plans, "would provide terrorists, both domestic and international, with (a) blueprint for undermining America's infrastructure and would jeopardize our nation's physical security."

Senator Lott advised the EPA that before moving forward "other federal agencies need to thoroughly review this plan—especially agencies responsible for monitoring and countering terrorist activities." He noted his expectation that the EPA would "submit this program to Congress for review prior to making an announcement."[10]

Similar sentiments have been expressed by other congressional leaders. Congressman Sherwood Boehlert (R-New York), a member of the House Permanent Select Committee on Intelligence, stated

that the EPA "failed to strike a proper balance" between the public's right to know and safeguarding national security.[11] Representative Charles W. Stenholm (D-Texas) complained to Carol Browner that worst case scenario data "not only provides terrorists with the tools for planning an attack but would also advise them on how to maximize the destructive force of an attack." He asserts that disclosure of this data "would have the effect of drawing a bull's-eye on manufacturing facilities all over the United States."[12] Congressman Stenholm is not wildly speculating about domestic terrorism. In his district, four members of the Ku Klux Klan attempted to blow up a natural gas processing facility.

The EPA and Computer Security

Although there are very few certainties in life, it is virtually certain that computer data is never totally secure. As U.S. Deputy Defense Secretary John Hamre observed, "The Internet was never designed with security in mind."[13] The Department of Defense penetrated its own computers when it tested its system's security with an unannounced hacker attack. If the nation's military security can be compromised, how securely will the EPA maintain corporate information?

James Makris, EPA director of chemical emergency preparedness and prevention, claims that EPA is "putting up speed bumps"[14] to help safeguard the data. These safeguard plans include limiting the number of facilities analyzed on any Internet site to 1,000 and requiring password protection for access to worst case scenario plans.

As any driver can attest, speed bumps may slow you down, but they are no barrier to access. Can anyone possibly think that passwords and multiple sites will actually deter terrorists?

The EPA appears to be incredibly nonchalant regarding the national security threat and the concerns of the intelligence community. Speaking before the District of Columbia Bar Association's Environment, Energy and Natural Resources Sec-

tion meeting, Mr. Makris remarked "The last time I checked we didn't need the security agencies 'approval' (to make decisions)."[15]

This nonchalance is not due to lack of awareness of the threat of terrorism from EPA Internet disclosure. A report by an EPA contractor revealed that putting worst case scenario data on the Worldwide Web would increase the risk of terrorism seven fold.[16] The study revealed that the EPA's gathering and disseminating targeting-quality data would make intelligence operations against the United States easier.

In light of this obvious threat, why would the EPA persist in pushing for Internet disclosure? One possible motive might be to chill firms' use and production of a variety of chemicals and other substances. EPA officials "point out that previous posting of chemical information on the Internet prompted companies to cut back use of hazardous materials."[17]

Even the inspector general of the EPA has determined that the agency "is not sufficiently protecting its information technology resources from malicious acts via access from the Internet."[18] The inspector general's report warned of intruders infiltrating Internet sites to penetrate security systems and to steal valuable information. Finally, the inspector general concluded that EPA "has not sufficiently developed or implemented adequate controls to prevent or detect improper/illegal access to its systems from the Internet."[19]

Even the inspector general of the EPA has determined that the agency "is not sufficiently protecting its information technology resources from malicious acts via access from the Internet."

Sadly, EPA has a poor record of safeguarding computer data. The agency recently reported losing 219 confidential business documents.[20] This loss comes on the heels of a 1996 admission that it

had lost more than 200 confidential and sensitive business reports. According to an internal EPA memorandum, the incident could be "an embarrassment to the agency which could damage our reputation and put into question our ability to handle sensitive information."[21] These security breakdowns add to concern about leaving the EPA responsible for safeguarding such data.

Economic Espionage and Internet Disclosure

Upon signing the Economic Espionage Act of 1996, President Clinton stated,

> Trade secrets are an integral part of virtually every sector of our economy and are essential to maintaining the health and competitiveness of critical industries operating in the United States. Economic espionage and trade secret theft threaten our nation's national security and economic well being.[22]

Expanded Internet disclosure by the EPA of business data will increase the threat of industrial or economic espionage.

The FBI defines economic espionage as "foreign-sponsored or coordinated intelligence activity directed at the United States or U.S. corporations, establishments, or persons for the purpose of unlawfully obtaining proprietary economic information."[23] As the leader in intellectual property—and public disclosure of proprietary business data—the United States is the number one target of industrial spies.

Many of these efforts are directed by the intelligence agencies of our trading partners. FBI Director Louis Freeh quotes a former German intelligence chief who made the following confession on German television, "It is true that for decades the state regulated the markets to some extent with its left hand while its right hand used the secret services to procure information for its own firms."[24]

Director Freeh reports that "current FBI investigations reflect 23 countries engaged in economic

espionage activities against the United States." One survey determined that 57 nations were actively engaged in economic espionage operations against U.S. firms while 100 countries were engaged in gathering proprietary economic information.[25]

Current foreign intelligence operations against U.S. firms involve many sectors of our economy, including telecommunications, aerospace, energy, transportation, and chemicals. Foreign economic espionage targets a host of proprietary business information ranging from bid, contract, customer, and strategy information to trade secrets. These espionage activities have noneconomic implications as well. According to FBI Director Freeh, "Collection of sensitive foreign economic intelligence frequently enhances a nation's military, as well as economic, capabilities."[26]

FBI Director Louis Freeh reports that "current FBI investigations reflect 23 countries engaged in economic espionage activities against the United States."

The amount of damage caused by economic espionage is difficult to quantify. As with other crimes, economic espionage often goes unreported because many victims are unwilling to share the degree of damage inflicted with shareholders and customers. A 1992 survey by the American Society for Industrial Security determined that economic espionage activities in 1991 though 1992 cost American firms billions of dollars in damages. Losses in pricing data were $1 billion. Product development and specification data and manufacturing process information damages were $597 million and $110 million, respectively.[27] According to the White House Office of Science and Technology, estimated losses to U.S. firms from economic espionage were nearly $100 billion.[28]

Open Source and Economic Threat

Economic espionage is not limited to James Bond-like or other sophisticated superspy techniques. Much of economic espionage activity involves obtaining data from open source materials made available from U.S. government agencies. Although obtaining and analyzing data from open sources is not within the technical definition of espionage, many intelligence agencies are engaging in gathering this data which, according to FBI Special Agent Edwin Fraumann, "can also serve to increase economic competitiveness."[29]

The National Counterintelligence Center's (NACIC) Annual Report to Congress on Foreign Economic Collection and Industrial Espionage in 1995 determined "open source information has increasingly been exploited by many foreign entities, to include foreign intelligence services in an attempt to target the United States."[30] The reasons for utilizing open-source collection as a form of economic espionage is obvious: open-source data is cheap to collect, widely available, and generally legal to obtain and use.

With the explosion of Internet usage and reporting requirements under expanded right to know, foreign competitors can obtain business data on specific American firms with ease. According to the NACIC, "foreign collectors have increased their direct connections with Internet service providers."[31] The Internet is the "fastest-growing" technique for foreign firms to obtain sensitive business data.[32] The anonymity and ease of use of the Internet makes it incredibly simple for industrial spies or terrorists alike to obtain open-source data.

Indeed, if industrial spies prefer to use an indirect route to obtain U.S. competitor information, the Environmental Defense Fund (EDF) has imported the EPA information to its site. Within minutes one can access the EDF page anonymously and obtain detailed reports on chemicals being used at more than 17,000 facilities across the country as well as maps pinpointing the firms' locations. The

data on the webpage comes from EPA's Toxics Release Inventory (TRI), providing information on 650 chemicals produced or used by U.S. manufacturers.

A few additional keystrokes take the would-be industrial spy to the EPA webpage and then to "Envirofacts." This webpage includes analysis of TRI data. By entering a zip code or city name the user is presented with a dazzling array of data including the names and addresses of firms as well as a list of the chemicals used or produced at the site. The EPA webpage also lists the names and addresses of offsite transfer recipient facilities and, as an added bonus, provides maps to each facility discussed.

Both the EPA and Environmental Defense Fund collect and make this data available to inform the public of potential health risks. However, as recognized by Professor Mary J. Culnan, a member of Presidents Clinton's Commission on Critical Infrastructure Protection,

> Once information gets on the Internet it can be manipulated in ways that were previously unfeasible and there is little accountability for how it is used. The more information that is made available, the more likely it will be used in ways that have nothing to do with the original reasons for collecting it.[33]

A study commissioned by the Chemical Manufacturers Association and performed by Kline & Company, a competitive intelligence firm, determined that data which would be disclosed publicly under an expanded right to know could be used by competitors to determine a target firm's manufacturing costs, probable technical advances, economic breakpoints, specific manufacturing processes, probable expansion plans, competitive strength, pricing flexibility, and the scale and efficiency of operations.[34] The risk to competitiveness from disclosure of this data is obvious. Nancy Ekart of Eastman Chemical Company predicts that "our foreign competitors are going to figure out what our cost structures are, our margins, and they can undercut us."[35]

Additionally, some manufacturers question the

usefulness of the data collected and disseminated, particularly in light of the threat of economic espionage. David Harpole of Lyondell Petrochemical Company says the additional data "will produce a number with no meaning." The initial intent of toxic release data was to document the release of chemicals into the environment, but the expanded reporting provides information on use and storage of materials that, when properly used, are never released.

The risk to competitiveness from disclosure of this data is obvious. ..."our foreign competitors are going to figure out what our cost structures are, our margins, and they can undercut us."

Similarly, Arco Chemical spokesman Ben Shuster questions the "usefulness of programs that require collection and broad dissemination of industry product or operating information that...don't really tell the public what they want to know."[36]

Internet disclosure of RMP and TRI data also undermines the Economic Espionage Act of 1996.[37] This statute criminalizes economic espionage and the theft of trade secrets. The act is designed to deter intrusive acts, such as hacking into a firm's database and stealing proprietary business information. However, to be subject to the sanctions of the act, the information must not be generally known or readily ascertainable by the "public." Internet disclosure provides more opportunities for competitors intelligence activities with no fear of criminal prosecution. The problem with disclosure under right to know is not limited to the EPA. Some states have adopted versions of right to know. Materials accounting programs implemented in Massachusetts and New Jersey include analysis of operations reporting chemicals under TRI. The states assert that the reporting has led to a decline in chemical use

and emissions. These conclusions have been questioned. A CMA study of the state programs asserts that the decline in emissions was due to economic factors that led to plant closures and a change in product mix.[38]

We have seen states, however, recognize the folly of these policies and the potential negative impacts they bring to businesses. New Jersey has removed 2,000 chemicals from its right to know program reporting list.[39] Recently, the state rejected an effort by a labor and environmental coalition to expand the number of chemicals to be reported under the New Jersey right to know program.[40]

Comparative Disclosure of Business Information

When evaluating a regulatory scheme, it is often helpful to employ a comparative approach to see how our neighbors and allies deal with similar problems. Not surprisingly, the United States offers the least amount of protection and the greatest degree of dissemination of business data in the industrialized world. Germany, Holland, Japan, Norway, Great Britain, and Sweden are comparable to the United States in levels of industrialization, regulatory systems, and political freedoms. Yet, the United States places a higher burden on firms claiming confidentiality in business information than do our trading partners. Of the other comparable nations, only Great Britain maintains a public inventory of chemical releases (like the TRI).

A European Union version of the TRI is in the works. Pursuant to European Union Directive 96/61/EC, "an inventory of the principal emissions and sources responsible shall be published every three years by the Commission on the basis of data supplied by the Member States."[41] Swedish firms' emissions data are published annually while Holland publishes a yearly study on emissions.

The Organisation for Economic Co-operation and Development (OECD) is also planning to join in the reckless rush to expand right to know. An OECD Draft Recommendation of the Council on

Environmental Information states:

> (A)ll relevant environmental information should be provided to any natural or legal person, in response to any reasonable request, without that person having to prove an interest, without unreasonable charges and as soon as possible, taking into account protection of privacy, industrial and commercial confidentiality, national security or other legitimate causes provided under national law.[42]

The OECD draft recommendation can be traced to Principle 10 of the 1992 Rio Declaration on Environment and Development. The principle states that "each individual shall have appropriate access to information concerning the environment that is held by public authorities."[43] Yet the Rio Declaration provided no steps for disclosure and was signed before widespread use of the Internet. No one could have predicted at the time of this declaration that environmental data would be available globally, in millions of homes, to anonymous users. The disclosure envisioned at the time of Rio was more akin to the Freedom of Information Act, which requires that an individual make a written request to obtain possibly sensitive information.

Conclusion and Recommendations

We are fortunate to live in a free and open society. Openness and disclosure promote efficiency and dialogue, which lead to informed debate and decision making. However, we have never assumed that we should surrender our national security or corporate proprietary information in the name of open disclosure, particularly not disclosure to anonymous users on the Internet.

Surveys reveal that Americans support U.S. firms in the fight to protect confidential business information. In a poll undertaken for the CMA by the Charlton Research Company, a whopping 96 percent of those polled felt that U.S. companies have

a right to protect sensitive business data. Although the survey indicated strong support for the EPA making TRI data publicly available (80 percent), the numbers dropped precipitously when those polled were informed of the threat of economic espionage via Internet disclosure. Three-fifths of those polled opposed disclosing TRI data to foreign competitors via the Internet.[44]

We live in a very different world than we did at the time of the passing of the Clean Air Act amendments. In 1990, domestic terrorism was limited to the silver screen and easily dealt with by Chuck Norris or Sylvester Stallone. The expanded right to know in the Clean Air Act amendments predated the explosive growth of the Internet, as well as the World Trade Center and Oklahoma City terrorist attacks. One FBI official doubted whether the risk management program of the Clean Air Act "would pass through Congress today, especially following the terrorist incidents in recent years and the issuance of the Weapons of Mass Destruction Act."[45]

Clearly there is a serious economic and national security threat from indiscriminate Internet disclosure of business data under TRI and RMP. Any plan to disclose this data should be done with the approval of the intelligence community in order to safeguard national security. The Departments of State and Commerce and the U.S. Trade Representative should also be involved in the decision making to protect American business interests.

Furthermore, in the spirit of open disclosure, a dialogue between environmentalists, government officials, and business leaders must search for a balanced approach towards disclosure. It is possible to develop a plan for disclosure that provides for the public's right to know and protects confidential business communication. This plan must balance the risk of environmental hazards, the threat of terrorism and economic espionage, the value and strategic importance of the data to be protected, and the need for safeguards. Only by constructive dialogue can we achieve this balance.

Notes

1. 40 Code Federal Register, Part 68; "Accidental Release Prevention Requirements: Risk Management Programs Under the Clean Air Act, Section 112(r)(7)," *Federal Register* 61, no. 120 (20 June 1996): p. 31715
2. "Internet chemical hazard data seen a threat," *Chemical Business Newsbase*, 13 March 1997 [available on nexis; news library].
3. Aegis Research Corp., ICF Inc., and Science Applications International Corp., "Security Study: An Analysis of the Terrorist Risk Associated With the Public Availability of Offsite Consequence Analysis Data Under EPA's Risk Management Program Regulations," (prepared for the United States Environmental Protection Agency, 7 December 1997), p. 7. *Chemical Market Reporter*, (27 April, 1998).
4. Julia Malone, "EPA's Internet Plan raises questions," *Austin American Statesman*, 30 May 1998, p. A8.
5. Ibid.
6. Ibid.
7. Knut Royce, "Worried About A What-If: Chemical Worst-Cases: Should They Be On Net?," *Newsday*, 10 May 1998, p. A24.
8. Traci Watson and Gary Fields, "Security Experts upset by EPA plan to post disaster data on Net," *USA Today*, 17 April 1998, p. A1; "EPA: Security Community Riled Over Internet Plan," *Greenwire*, 17 April 1998.
9. "New Analysis Examines Terrorist Threat to U.S.; Warns Nature, Form of Terrorism are Evolving," *PR Newswire*, 17 April 1998 [available on Nexis; news library].
10. Senator Trent Lott (R-Mississippi), letter to Carol M. Browner, administrator of the United States Environmental Protection Agency, 17 February 1998.
11. Representative Sherwood Boehlert (R-New York), letter to Carol Browner, administrator of the U.S. Environmental Protection Agency, 17 February 1998.
12. Rep. Charles W. Stenholm (D-Texas), letter to Carol Browner, administrator of the U.S. Environmental Protection Agency, 3 March 1998.
13. Alexander Nicoll and Louise Kehoe, "U.S. Warns of Risks Internet Poses to National Security," *Financial Times*, 20 March 1998, p. 22.
14. Ibid.
15. Jim Makris, U.S. Environmental Protection Agency, "Terrorist Risk vs. Right to Know: Internet Access to Chemical Release Data," remarks to the District of Columbia Bar Association Environment, Energy and Natural Resources

Section, 13 March 1998.

16. Aegis Research Corporation, ICF Inc., and Science Applications International Corporation, "Security Study: An Analysis of the Terrorist Risk Associated With the Public Availability of Offsite Consequence Analysis Data Under EPA's Risk Management Program Regulations," (prepared for the United States Environmental Protection Agency, 7 December 1997), p. 7. *Chemical Market Reporter* (27 April 1998).
17. "EPA: Security Community Riled Over Internet Plan," *Greenwire*, 17 April 1998.
18. Office of the Inspector General of the U.S. Environmental Protection Agency, "EPA's Internet Connectivity Controls," Report No. 7100284 (September 1997), p. 8.
19. Ibid. p. 5.
20. "EPA Lost 400 Confidential U.S. Chem Files," *Chemical News and Intelligence* (27 February 1998).
21. "EPA Loses Confidential Chemical Files: Mistakes Calls into Question the Agency's Ability to Manage Chemical Use Information," *Chemical Market Reporter*, November 18, 1996, p. 6.
22. President Clinton, statement upon signing the Economic Espionage Act of 1996, 11 October 1996.
23. Federal Bureau of Investigation, "Economic Espionage and Protection of Proprietary Economic Information Act of 1996," Federal Bureau of Investigation Proposal, 4 December 1995.
24. Louis J. Freeh, statement before the Senate Select Committee and Senate Committee on the Judiciary, Subcommittee on Terrorism, Technology and Government Information, Hearing on Economic Espionage, 104th Cong., 2nd Sess., 28 February 1996.
25. Edwin Fraumann, "Economic Espionage: Security Missions Redefined," *Public Administration Review* 57, no. 4 (July/August 1997), p. 304.
26. Louis J. Freeh.
27. Jack Nelson, "Spies Took $300 Billion Toll on U.S. Firms in 97," *Los Angeles Times*, 12 January 1998, p. 1.
28. Senator Arlen Specter (P-Pennsylvania), statement in hearing on economic espionage before the Senate Select Committee on Intelligence, 104th Cong., 2nd Sess., 28 February 1996.
29. Fraumann.
30. National Counterintelligence Center (NACIC), *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*, 104th Cong., 2nd Sess., 1995.
31. Ibid.

32. "Internet: The Fastest Growing Modus Operandi for Unsolicited Collection," *NACIC Counterintelligence News and Development Newsletter* 4 (November 1996), http://www.NACIC.gov/cind/cindov.htm#art2, June 5, 1997.

33. Mary J. Culnan, "What is Plain to See...," *Washington Post*, 13 July 1997, p. D1.

34. Kline & Company, *Impact of Proposed TRI-Phase 3 Reporting Requirements on Intellectual Property Protection*, final report to the Chemical Manufacturers Association (2 November 1995); "Economic Espionage: The Looting of America's Future in the Information Age," *Chemical Manufacturers Association* (Winter 1998), pp. 30-31.

35. Chris Woodyard, Planned Disclosure rules worry chemical makers, Houston Chronicle, November 2, 1996, p. 1.

36. Ibid.

37. *Economic Espionage Act of 1996*, Public Law 104-294, 110 Stat. 3400 (1996.)

38. "TRI: CMA Study Questions States Success with Toxic Use Reduction Programs," *Hazardous Waste News* (22 December 1997), available on Nexis; News Library.

39. Rick Mullin, "New Jersey's Take on Industry," *Chemical Week*, (10 September 1997), p. 3.

40. Bruno Tedeschi, "State Rejects Group Request to Expand Right to Know List," The Record (28 May 1998), available on Nexis; News Library.

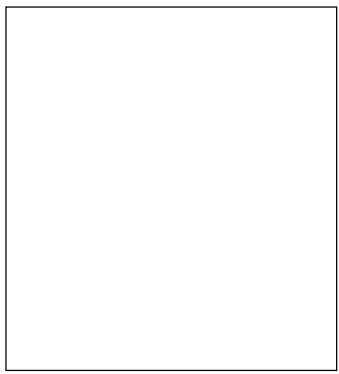
41. "Council Directive 96/61/EC concerning integrated pollution prevention and control," *Official Journal of the European Communities* L257/26 (1996).

42. Council on Environmental Information of the Organisation for Economic Co-operation and Development, draft recommendation, May 1997.

43. United Nations Conference on Environment and Development, *Rio Declaration on Environment and Development*, 14 June 1992.

44. Charlton Research Company, *National Issues Survey* (May 1997).

45. Rick Shapiro, Federal Bureau of Investigation, remarks in the summary of a meeting of the Accident Prevention Subcommittee, *EPA* (3 February 1998), p. 4.



William H. Lash III is a Distinguished Senior Fellow of the Center for the Study of American Business at Washington University in St. Louis. Professor Lash has testified before congressional committees and spoken to numerous trade associations and research institutes on issues of foreign investment and international trade. His articles on international trade and corporate law have appeared in ***The Wall Street Journal****,* ***The Washington Times****, and leading law journals. He is also the author of* ***State and Local Trade Sanctions: A Threat to U.S. Interests****, an earlier title in this series.*

Additional titles in this series are available on our website at http://csab.wustl.edu or by contacting CSAB.

Center for the Study of American Business
Washington University
Campus Box 1027
One Brookings Drive
St. Louis, MO 63130-4899
Phone (314) 935-5630

Washington
WASHINGTON UNIVERSITY IN ST. LOUIS