American University Law Review

Volume 53 | Issue 1 Article 4

2003

The Freedom of Information Act Post-9/11: Balancing the Public's Right to Know, Critical Infrastructure Protection, and Homeland Security

Kristen Elizabeth Uhl

The Freedom of Information Act Post-9/11: Balancing the Public's Right to Know, Critical Infrastructure Protection, and Homeland Security

Keywords
Freedom of Information Act, 9/11, post-9/11, Homeland security, Department of Justice, Homeland Security Act of 2002, Public safety, Public-Private information

COMMENT

THE FREEDOM OF INFORMATION ACT POST-9/11: BALANCING THE PUBLIC'S RIGHT TO KNOW, CRITICAL INFRASTRUCTURE PROTECTION, AND HOMELAND SECURITY

KRISTEN ELIZABETH UHL*

TABLE OF CONTENTS

* Managing Editor, *American University Law Review*, Volume 53; J.D. Candidate, May 2004, *American University, Washington College of Law*; B.S.F.S., 2000, *Georgetown University*. I would like to thank my parents, Sam and Donna Uhl, for their loving support and patience. I am grateful to Professor Robert G. Vaughn for sharing his expertise on the Freedom of Information Act. I would also like to thank Stephanie Quaranta, Rebecca Troth, Roy E. Brownell II, and the members of the *American University Law Review* for their invaluable editorial assistance. Last but not least, I could not have written this Comment without Loren Southard's insight and unending encouragement. Thank you all for making my dream of publication a reality.

INTRODUCTION

Public access to government information is one of our nation's most cherished and established principles.[1] Yet in times of war,[2] this and other freedoms are often eclipsed in favor of competing government interests.[3] Americans have come to expect a degree of transparency in their government: for nearly forty years, the Freedom of Information Act ("FOIA")[4] has entitled the public to obtain certain information through mandatory government disclosures. However, the United States government, with President

1. In signing the Freedom of Information Act ("FOIA") into law, President Lyndon B. Johnson declared, "[t]his legislation springs from one of our most essential principles: [a] democracy works best when the people have all the information that the security of the Nation permits." H. REP. NO. 104-795, at 8 (1966), *cited in* Paul M. Schoenhard, Note, *Disclosure of Government Information Online: A New Approach From an Existing Framework*, 15 HARV. J.L. & TECH. 497, 499 (2002).

2. President Bush commented, "[w]e're an open society, but we're at war . . . . Foreign terrorists and agents must never again be allowed to use our freedoms against us." Brad Knickerbocker, *Security Concerns Drive Rise in Secrecy*, CHRISTIAN SCI. MONITOR, Dec. 3, 2001, at 1, *cited in* Schoenhard, *supra* note 1, at 503. "From Abraham Lincoln's suspension of the right of habeas corpus during the Civil War, to the internment of Japanese-Americans during World War II, to the surveillance of anti-Vietnam War protestors and civil rights leaders, we see that our freedoms and liberties are often sacrificed in times of conflict." Schoenhard, *supra* note 1, at 508 (citing Adam Cohen, *Rough Justice; The Attorney General Has Powerful New Tools to Fight Terrorism. Has He Gone Too Far?*, TIME, Dec. 10, 2001, at 30); *cf.* Stephen Gidiere & Jason Forrester, *Balancing Homeland Security and Freedom of Information*, 16 NAT. RESOURCES & ENV'T 139, 139 (2002) (noting that the September 11, 2001 terrorists "availed themselves of the everyday freedoms that Americans take for granted," such as purchasing an airline ticket over the Internet and enrolling in a pilot training course). Once information is released to the public, it may eventually fall into terrorists' hands. *Id.*

3. "The goal of an informed citizenry and open government is often at odds with other public interests," such as "maintaining an efficient and effective government," and the "preservation of the confidentiality of sensitive information." Jeffrey Norgle, Comment, *Revising the Freedom of Information Act for the Information Age: The Electronic Freedom of Information Act*, 14 J. MARSHALL J. COMPUTER & INFO. L. 817, 822 (1996) (tracing Freedom of Information Act ("FOIA") developments in response to public needs, citing 5 U.S.C. § 552(b)(1)-(9) (1988)). *See also Administrative Law, Adjudicatory Issues, and Privacy Ramifications of Creating a Department of Homeland Security: Hearing Before the Subcomm. on Commercial & Admin. Law of the House Comm. on the Judiciary*, 107th Cong. 2 (2002) (statement of Rep. Watt, Member, House Comm. on the Judiciary) (arguing that the government's goal of protecting its citizens "will involve sacrificing personal liberties"); Laura Parker et al., *Secure Often Means Secret*, USA TODAY, May 16, 2002, at 1A, 4A (reporting that "[t]he U.S. government often has embraced secrecy during crises," particularly during times of war); Robert L. Saloschin, *The Department of Justice and the Explosion of Freedom of Information Act Litigation*, 52 ADMIN. L. REV. 1401, 1407 (2000) (arguing that when the public must be protected from "ruthless adversaries, even the perception of openness in government can be devastating"); Laura A. White, Note, *The Need for Governmental Secrecy: Why the U.S. Government Must Be Able to Withhold Information in the Interest of National Security*, 43 VA. J. INT'L L. 1071, 1079 (2003) (citing Michael Kelly, *Secrecy, Case by Case*, WASH. POST, Aug. 28, 2002, at A23, and arguing that democratic ideals must occasionally be offended in order for the United States to maintain national security and freedom).

4. 5 U.S.C. § 552 (2002).

George W. Bush and Attorney General John Ashcroft at the helm, recently set in motion mechanisms that will restrict the flow of government information to the requesting public.[5]

As the horror of al Qaeda's September 11, 2001 attack still haunts the nation's consciousness, the U.S. remains a target for terrorist groups.[6] Despite a massive effort to eliminate terrorist networks, national security experts argue that the U.S. is just as vulnerable to attack as it was on September 10, 2001.[7] Although scattered, the al Qaeda network may remain capable of terrible attacks despite our efforts.[8]

While the U.S. government attempts to strengthen national security to meet this evolving threat, a re-examination of some of our country's core values and principles is an entirely proper public response.[9] In particular, one must examine whether our government's high degree of transparency, though serving a valuable social purpose, may also provide support to terrorists.[10] Although

5. *See* discussion *infra* Parts II & III (reviewing FOIA developments post-September 11, 2001).

6. *See* Dan Eggen, *Risk of Terror Attack Climbs, U.S. Finds*, WASH. POST, Feb. 6, 2003, at A10 (reporting senior U.S. intelligence officials' conclusions that the risk of terrorist attacks on U.S. soil has increased significantly); *see also* THE WHITE HOUSE, THE NATIONAL STRATEGY FOR THE PHYSICAL PROTECTION OF CRITICAL INFRASTRUCTURES AND KEY ASSETS 7 (2003) [hereinafter NSPPCIKA] (arguing that our enemies "consider terrorism an effective weapon to use against us, and they will continue to employ such tactics" until the U.S. can prove it is no longer effective).

7. *See* Barton Gellman, *In U.S., Terrorism's Peril Undiminished*, WASH. POST, Dec. 24, 2002, at A01, A06 (quoting a Bush insider as stating that "[w]ith untold billions spent—money, personnel and blood—how can we claim any kind of success if we're just as vulnerable as before?"); *see also* COUNCIL ON FOREIGN RELATIONS, AMERICA—STILL UNPREPARED, STILL IN DANGER 13 (2002) (reporting that a year after September 11, America remains dangerously unprepared to prevent and respond to a terrorist attack on U.S. soil), *available at* http://www.cfr.org/pdf/Homeland_TF.pdf (on file with the American University Law Review). In all likelihood, the next attack will result in a large number of casualties and widespread disruption to American lives and the economy. *Id.*

8. Gellman, *supra* note 7. As it did with box cutters and jetliners on September 11, 2001, al Qaeda could make innovative use of ordinary technology to attack the U.S. *Id.* Of particular concern to security experts is the possibility of undiscovered "sleeper cells" on U.S. soil. *Id.*

9. *See* Marc Rotenberg, *Privacy and Secrecy After September 11*, 86 MINN. L. REV. 1115, 1116, 1124 (2002) (commenting on the expansion of "government secrecy," including the denial of public access to government information post-September 11, 2001). In reconsidering our core freedoms, debate has swirled around FOIA because al Qaeda groups in Afghanistan were found with copies of General Accounting Office reports and other government information obtained through FOIA. *See* 148 CONG. REC. H5828-06 (daily ed. July 26, 2002) (statement of Rep. Davis) [hereinafter Statement of Davis] (arguing that while the United States works to protect national security against terrorism, "we also need to ensure that we are not arming terrorists").

10. *See, e.g.*, *Homeland Security Efforts: Hearing Before the House Comm. on Science*, 107th Cong. 32 (2002) (statement of James K. Kallstrom, Special Advisor to Governor Pataki on Counter-Terrorism) [hereinafter Statement of Kallstrom]

certain information disclosed under FOIA may be important for public safety, other information obtained through FOIA could also put us at risk. In the past two years alone, public requests under FOIA have yielded important public safety information—from reports about excessive levels of mercury in canned tuna,[11] to details about the presence of anthrax spores in Washington, D.C.'s Brentwood mail facility.[12] However, the importance of this information must now be weighed against frightening new evidence that the U.S. military found al Qaeda groups in possession of U.S. General Accounting Office ("GAO") Reports and government information obtained through FOIA.[13] Specifically, investigators discovered "detailed maps and drawings of sensitive infrastructure locations" in caves in Afghanistan and in al Qaeda training camps.[14]

The U.S. government's knee-jerk reaction to such evidence was to restrict public access to government information in the name of national security.[15] The government accomplished this goal through agency guidance in new FOIA memoranda and through a broad FOIA exemption for the new Department of Homeland Security. Although these recent FOIA developments did not receive much attention from the mainstream news media,[16] Americans will be shocked to realize the practical implications of losing their right to enjoy free and open access to government information.[17]

(arguing that new FOIA legislation must ensure that "sensitive information about potential threats to the Nation's critical infrastructure" must not "fall into the wrong hands" and be used to attack us); THE WHITE HOUSE, THE NATIONAL STRATEGY FOR HOMELAND SECURITY 56 (2002) [hereinafter NSHS] (arguing that while it is important to protect public access to government information, that right must be balanced against protecting national security).

11. The National Security Archive, *The U.S. Freedom of Information Act at 35: Nearly 2 Million Requests Last Year at a Cost of One Dollar Per Citizen; National Security Archive Electronic Briefing Book Number 51* [hereinafter FOIA at 35], *at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB51/ (last visited Oct. 11, 2003) (on file with the American University Law Review).

12. *See Judicial Watch Files Criminal Complaint With U.S. Attorney Roscoe C. Howard Over Brentwood Anthrax Cover-Up* (Dec. 6, 2002) [hereinafter Anthrax Lawsuit] (detailing information disclosed in a FOIA request that U.S. Postal Service and U.S. government officials knew four days before closing the Brentwood mail facility that envelopes had leaked anthrax spores, putting the employee population at risk), *at* http://www.judicialwatch.org/2817.shtml (on file with the American University Law Review).

13. Statement of Davis, *supra* note 9.

14. Statement of Kallstrom, *supra* note 10.

15. *See* discussion *infra* Parts II & III (reviewing the reduction of FOIA disclosures in the past year).

16. *See infra* notes 249-50 (discussing the media's lack of coverage of FOIA developments in the past year).

17. *See* discussion *infra* Part IV.C (discussing the practical implications of the Department of Homeland Security FOIA exemption).

These efforts to erode FOIA will only provide a false sense of security at the expense of the public's right to information. This new framework broadens the preexisting FOIA exemption framework, is largely unnecessary, and may even endanger public safety.[18] Congress has already carved out FOIA exemptions in 5 U.S.C. § 552 in order to safeguard sensitive records, without the severe limitations imposed by the new FOIA guidelines.[19]

This Comment will reexamine the spirit and purpose behind FOIA, arguing that the American public's right to governmental transparency, conceived during the national security crises of the Cold War, is as vital today as it was nearly four decades ago. Part I of this Comment will examine FOIA's history and mechanics. Part II will address the role of the Department of Justice ("DOJ") in shaping agency decisions in the FOIA request process and assess the roles that key figures in the Bush Administration play in restricting the availability of government information post-September 11, 2001. Part III will trace the development of the new Department of Homeland Security and evaluate the broad FOIA exemption applicable to this new cabinet-level department. Finally, Part IV will argue that recent FOIA developments will restrict public access to government information, and that these new policies are unnecessary in light of the preexisting FOIA exemption framework under 5 U.S.C. § 552. In sum, this Comment concludes that FOIA developments in the aftermath of September 11, 2001 have created a climate of nondisclosure, and that the "war against terrorism" does not justify the magnitude of recent data restrictions imposed by the U.S. government.

I. THE FREEDOM OF INFORMATION ACT'S HISTORY AND MECHANICS

Enacted in 1966,[20] FOIA was the first federal law to establish an effective legal right of access to government information on the basis of openness and accountability.[21] Before FOIA, the public bore the

18. *See* discussion *infra* Part IV.C.1 (describing how the Department of Homeland Security FOIA exemption broadens the preexisting FOIA exemption framework).

19. *See* 5 U.S.C. § 552(b)(1)-(9) (2002).

20. Congress passed FOIA "in the late 1960s, during the apparent stalemate in the Vietnam War—an event that stimulated popular distrust of government." Saloschin, *supra* note 3, at 1401.

21. *See* Scott A. Faust, Note, *National Security Information Disclosure Under the FOIA: The Need for Effective Judicial Enforcement*, 25 B.C. L. REV. 611, 643 & n.3 (1984) (quoting Senator Long's comments prior to the enactment of FOIA that "our purpose in introducing [FOIA] is that a necessary corollary to the right of a democratic people to participate in governmental affairs is the right to acquire information," 111 CONG. REC. S2797 (daily ed. Feb. 17, 1965)).

burden of demonstrating a right to access government records.[22] Now, however, FOIA grants the public a "right to know" standard for access to government information, shifting the burden of proof from the public to the government agency seeking to deny access.[23] FOIA has become one of the primary means by which the public informs itself about its government, and it has been used to obtain information crucial to the public interest.[24] Recently, for example, public use of FOIA exposed information on the National Aeronautics and Space Administration's projected $4 billion cost overrun for the international space station and how prescription rates for Ritalin varied from region to region.[25] Following the U.S.'s lead, laws instituting FOIA's principles of transparency in government have spread across the globe.[26]

Congress amended FOIA four times between 1974[27] and 1996.[28] The amendments between 1974 and 1986 changed certain procedures, modified exemptions, protected sensitive law enforcement information, and created new fee provisions.[29] The 1996 amendment, known as the Electronic FOIA ("EFOIA")

22. GENERAL ACCOUNTING OFFICE, INFORMATION MANAGEMENT: UPDATE ON THE IMPLEMENTATION OF THE 1996 ELECTRONIC FREEDOM OF INFORMATION ACT AMENDMENTS 4 (2002) [hereinafter GAO], *available at* http://www.fas.org/sgp/foia/gao02493.pdf (on file with the American University Law Review). FOIA replaced the disclosure provisions of the Administrative Procedure Act of 1946, which required the government to withhold material requiring secrecy in the public interest or material pertinent only to the internal affairs of an agency. Administrative Procedure Act of 1946, Pub. L. No. 79-404, 60 Stat. 237 (1946). The ultimate effect of this legislation was to limit the amount of information the government needed to disclose to the public. *See* Schoenhard, *supra* note 1, at 498 (discussing the widely-held view that the Administrative Procedure Act actually limited public access to government information).

23. GAO, *supra* note 22, at 4.

24. *See* Thomas Blanton, *The World's Right to Know*, FOREIGN POL'Y, July 1, 2002, at 50 (reporting that FOIA is the world's most heavily invoked disclosure law).

25. FOIA at 35, *supra* note 11. In the past, public requests under FOIA led to the disclosure of such controversial information as Army reports concerning the massacre at My Lai. *See* John Moon, *The Freedom of Information Act: A Fundamental Contradiction*, 34 AM. U. L. REV. 1157, 1175 (1985) (citing N.Y. TIMES, Apr. 4, 1972, at 7, col. 1).

26. In particular, the past decade has witnessed an expansion in governmental transparency worldwide. *See* Blanton, *supra* note 24, at 50 (reporting that in the past decade, twenty-six countries, including Bulgaria, South Africa, Thailand, and Japan, enacted disclosure statutes guaranteeing the right of access to government information). In light of these developments, it is ironic that "secrecy has made the most dramatic comeback" in the U.S.—the country that initially led the shift toward government transparency. *Id.*

27. The Watergate scandal "intensified disclosure efforts and led to the 1974 amendments strengthening FOIA." Saloschin, *supra* note 3, at 1404 (citing Pub. L. No. 93-502, 88 Stat. 1561 (codified as amended at 5 U.S.C. § 552 (1994))).

28. GAO, *supra* note 22, at 4.

29. *Id.*

amendment,[30] effectively took FOIA to the Internet, requiring each agency to post on its website guides to making FOIA requests. Further, this amendment encouraged online public access to government information by requiring agencies to make certain information available in electronic form.[31] As a result, government websites thrived on the Internet.[32]

FOIA provides public access to agency records[33] through two methods: affirmative agency disclosure and public request for disclosure.[34] Affirmative agency disclosure takes place through the *Federal Register* publication of information ("the FOIA publication requirement") and the availability of certain records for public inspection and copying ("the FOIA reading room requirement").[35] Public request for disclosure, FOIA's most well-known component, allows any member of the public to request access to information held by federal agencies without showing a need or reason for seeking the information.[36]

Although the public has a statutory right to request government records, agencies are not always required to comply with FOIA requests. Through nine exemptions, FOIA balances the value of public disclosure against other important considerations, including

30. In response to lengthy delays and extensive request backlogs at agencies, Senator Patrick Leahy introduced amendments to FOIA for electronic records in 1994, eventually leading President Clinton to sign the Electronic Freedom of Information Act ("EFOIA") amendment in October 1996. The National Security Archive, *The FOIA and President Bill Clinton*, *at* http://www.gwu.edu/~nsarchiv/nsa/foia/clinton.html (last visited Oct. 11, 2003) (on file with the American University Law Review).

31. The EFOIA amendment encouraged online public access to government information by requiring agencies to make six specific types of records, created on or after November 1, 1996, available in electronic form. *See* GAO, *supra* note 22, at 8 (citing 5 U.S.C. § 552(a)(2)(A)–(E) and 5 U.S.C. § 552(e)(2)).

32. *See* Schoenhard, *supra* note 1, at 502 (surveying the availability of government information on agency websites).

33. "Agency records" are defined as "documents that (1) are either created or obtained by an agency and (2) are in that agency's physical possession and under its control at the time of the FOIA request." *A Blackletter Statement of Federal Administrative Law*, 54 ADMIN. L. REV. 17, 61-62 (2002).

34. GAO, *supra* note 22, at 4; *see also* Norgle, *supra* note 3, at 824 (listing the information that agencies are obligated to release under FOIA). "First, agencies must publish substantive rules, statements of general policy and information on agency organization and procedures in the Federal Register." *Id.* (citing 5 U.S.C. § 552(a)(1) (1998)). "Second, agencies must make final adjudicatory opinions, statements of policy not published in the Federal Register, and administrative staff manuals and instructions available for inspection and copying." *Id.* (citing 5 U.S.C. § 552(a)(2) (1998)). "Third, agencies must make available other records not falling within the first two categories." *Id.* (citing 5 U.S.C. § 552(b) (1998)).35.GAO, *supra* note 22, at 4.

36. *Id.*

national security and the protection of sensitive business information.[37] Rather than requiring agencies to withhold information subject to an exemption, agencies are granted discretion to determine whether to safeguard or disclose that information.[38] Moreover, FOIA does not provide access to records held by the U.S. Congress or the federal judiciary,[39] state or local government agency records, or those held by private businesses or individuals.[40] Each state and the District of Columbia have statutes governing public access to their records.[41] Finally, requesters dissatisfied with the amount of information they receive pursuant to an exemption may seek redress in the U.S. District Courts.[42]

In an effort to protect national security, recent government actions expanded the FOIA exemption framework and restricted the public's ability to access sensitive government information.[43] The Executive Branch, particularly the DOJ, has thus far played a key role in creating a new climate of nondisclosure whereby the public could be increasingly denied access to government information.

II. THE DEPARTMENT OF JUSTICE AND FOIA IMPLEMENTATION

A. Background

The DOJ plays an integral role in interpreting and developing FOIA, overseeing agencies' compliance with FOIA, defending agencies' decisions in court, and serving as the primary source of policy guidance for agencies.[44] The number of FOIA-related matters

37. 5 U.S.C. § 552(b)(1)-(9) (2002); *see* Joseph Summerill, *Is It Safe For Your Client To Provide The Government With Homeland Security Data?*, 50 FED. LAWYER 24, 26 (2003) (arguing that the exemptions indicate that sometimes the interest in protecting sensitive records outweighs the public interest of disclosure).

38. *See* Ronald Backes, Comment, *Freedom, Information, Security*, 10 SETON HALL CONST. L.J. 927, 976 (2000) (citing Chrysler Corp. v. Brown, 441 U.S. 281, 293 (1979)).

39. The National Security Archive, *About the Freedom of Information Act (FOIA), at* http://www.gwu.edu/~nsarchiv/nsa/foia/aboutfoia.html (last visited Oct. 11, 2003) (on file with the American University Law Review).

40. *Id.*

41. *Id.*

42. Judges determine the propriety of agency withholdings de novo and agencies must bear the burden of sustaining their nondisclosure actions. 5 U.S.C. § 552(a)(4)(B)-(C) (2002). *But see* Moon, *supra* note 25, at 1178, 1188 (citing disagreement over whether judges objectively apply FOIA, and concluding that "judicial construction of the FOIA is an exercise in subjectivity").

43. *See* discussion *infra* Parts II & III (reviewing FOIA developments in the Executive and Legislative branches post-September 11, 2001).

44. DOJ published a newsletter called *FOIA Update*, wrote *A Short Guide to the Freedom of Information Act*, and regularly issued an analytical Freedom Of Information Case List of court decisions in order to provide the government with a better

at DOJ exploded in the mid-1970s and has increased steadily.[45] The public submitted 1,965,919 FOIA requests to federal agencies in fiscal year 1999, and agencies processed 1,939,668 requests that same year.[46] Along with the massive number of requests came high levels of backlogs as agencies scrambled to meet the public's needs.[47]

Because DOJ plays such a critical role in shaping agency responses to FOIA requests,[48] several Attorneys General left their particular Administration's mark on FOIA policy.[49] The Attorney General traditionally issues a new FOIA policy statement at the beginning of a new Administration—at least when the incoming President has a different political affiliation from the former.[50] The various Administrations' approaches to FOIA are extremely important because they ultimately determine how DOJ attorneys will represent agency decisions to withhold information. The FOIA policies of the

---

understanding of FOIA. Saloschin, *supra* note 3, at 1404-05. In 2000, DOJ developed *FOIA Post*, a means of disseminating FOIA information to federal agencies that is located on the DOJ FOIA website at http://www.usdoj.gov/oip/foiapost/mainpage.htm (last visited Oct. 11, 2003) (on file with the American University Law Review).

45. Saloschin, *supra* note 3, at 1403. Saloschin, a former attorney in the DOJ's Office of Legal Counsel, argues that the reasons behind this expansion in FOIA-related matters included the "vigorous use of FOIA by Ralph Nader and his associates; the growing popularity of FOIA as a form of pre-trial discovery among litigators; the use of FOIA by various scholars, advocates, and authors; and the use of FOIA on behalf of businesses involved in publishing or in government procurement or regulation." *Id.* at 1401, 1403-04.

46. *See, e.g.*, FOIA at 35, *supra* note 11 (providing a summary of FOIA requests filed in fiscal year 1999). George Washington University's National Security Archive, the nation's primary non-profit FOIA user, also collects data pertaining to its own FOIA requests. *Id.*

47. For example, on one National Security Archive request filed in 1990, the Central Intelligence Agency took *nine years* to deny fully twenty-two documents, and another seven months to deny the National Security Archive's appeal. *Id. See, e.g.*, Saloschin, *supra* note 3, at 1404 (arguing that in the 1970s, "appeals to the Attorney General from initial denials of DOJ records skyrocketed from about six per year to approximately a thousand," leading to the creation of a new appeals office); GAO, *supra* note 22, at 42 (detailing the Department of Energy's median time to process a request in Fiscal Year 1999 as 250 days).

48. Saloschin writes that "[t]he DOJ must balance several functions that potentially conflict in FOIA work." Saloschin, *supra* note 3, at 1405. DOJ serves as the legal advisor to the government and litigates on behalf of almost all federal agencies. *Id.* However, because the DOJ is the government's "law enforcement arm," it must ensure agency compliance with all laws. *See id.* at 1405-06 (citing 5 U.S.C. § 552(e)(5) (1994 & Supp. IV 1998)). Therefore, conflicts may arise when DOJ performs more than one of these functions. Saloschin, *supra* note 3, at 1406.

49. *See* Norgle, *supra* note 3, at 825 (arguing that the Executive Branch under the Clinton Administration made an effort to further strengthen federal agency adherence to FOIA, citing *Administration Tells Agencies to Tilt Toward FOIA Disclosure*, 62 U.S.L.W. 15, 20 (1993)).

50. Such statements were issued in May 1977 by Attorney General Griffin B. Bell, in May 1981 by Attorney General William French Smith, in October 1993 by Attorney General Janet Reno, and in 2001 by Attorney General John Ashcroft. GAO, *supra* note 22, at 10.

Clinton and Bush Administrations provide an interesting study of contrasting approaches to government disclosures.

B. The Expansion of Disclosure Under the Clinton Administration

President William J. Clinton and Attorney General Janet Reno ushered in an era of increased FOIA disclosures through concurrent FOIA memoranda issued on October 4, 1993.[51] President Clinton's memorandum reaffirmed the value of a free and open society and asked agencies to "renew their commitment to [FOIA], to its underlying principles of government openness, and to its sound administration."[52] Attorney General Reno's memorandum further developed the Administration's concept of these principles, overturning the Reagan Administration's "substantial legal basis" threshold for agency defense and replacing it with a "presumption of disclosure."[53]

Specifically, Attorney General Reno's memorandum established a "foreseeable harm" standard, committing DOJ to defend an agency's decision to withhold information "only in those cases where the agency *reasonably foresees* that disclosure would be *harmful* to an interest protected by that exemption."[54] Reno further instructed agencies that "[w]here an item of information might technically or arguably fall within an exemption, it ought not to be withheld from a FOIA requester unless it need be,"[55] and stated that the principle of openness in government should be applied in "every disclosure and non-disclosure decision."[56] The Administration believed that this policy best served the public interest because it achieved FOIA's main objective—"maximum responsible disclosure of government information—while preserving essential confidentiality."[57] This policy

---

51. Memorandum from Janet Reno, Attorney General, to Heads of All Federal Departments and Agencies re: The Freedom of Information Act (Oct. 4, 1993) [hereinafter Reno Memorandum], *available at* http://www.usdoj.gov/oip/foia_updates/Vol_XIV_3/page3.htm (on file with the American University Law Review).

52. Memorandum from William J. Clinton, President of the United States, to Heads of Departments and Agencies re: The Freedom of Information Act (Oct. 4, 1993) [hereinafter Clinton Memorandum], *available at* http://www.gwu.edu/~nsarchiv/nsa/foia/whinitial.pdf (on file with the American University Law Review). In handling requests, President Clinton petitioned agencies to handle requests for information in a "customer-friendly manner." *Id.*

53. Reno Memorandum, *supra* note 51. The memorandum also pointed out that many departments have backlogs due to fewer resources and heavy workloads, and identified this as a serious problem. *Id.*

54. *Id.* (emphasis added).

55. *Id.*

56. *Id.*

57. *See* Reno Memorandum, *supra* note 51 (justifying the Clinton Administration's presumption of disclosure).

remained in effect throughout the Clinton Administration, and agencies continued to follow this guidance until October 2001.[58]

C. The Erosion of FOIA Under the Bush Administration

The terrorist attacks on September 11, 2001 led the Bush Administration to rethink government policies toward disclosure of government information.[59] FOIA was not immune: Attorney General John Ashcroft introduced a new FOIA policy memorandum on October 12, 2001 ("Ashcroft Memorandum").[60] In the memorandum, Attorney General Ashcroft encouraged the protection of national security, sensitive business information, and personal privacy.[61] Specifically, the Ashcroft Memorandum assured agencies that "the Department of Justice will defend your decisions unless they lack a *sound legal basis* or present an unwarranted risk of adverse impact on the ability of other agencies to protect other important records."[62] This memorandum officially replaced the Clinton Administration's "foreseeable harm" standard with a new "sound legal basis" standard governing DOJ's defense of FOIA lawsuits.[63]

---

58. *See* FOIA POST, *New Attorney General FOIA Memorandum Issued* (reporting that Attorney General Ashcroft's FOIA memorandum superseded the Clinton Administration's 1993 FOIA policy), *at* http://www.usdoj.gov/oip/foiapost/2001 foiapost19.htm (last visited Oct. 11, 2003) (on file with the American University Law Review).

59. *See, e.g.*, Press Briefing, The White House, The President's Announcement on Homeland Security (June 6, 2002) [hereinafter Homeland Defense Press Briefing] (asserting that "in times of crisis, we ask our leaders to do big things, to respond to the crisis"), *available at* http://www.whitehouse.gov/news/releases/2002/06/ 20020606-6.html (on file with the American University Law Review); Blanton, *supra* note 24 (arguing that it became apparent to our government that increased governmental secrecy could be a "crucial weapon in the war against terror"); Parker, *supra* note 3 (reporting a "dramatic turnabout from the policies of the past three decades," and that since September 11, 2001, "the Bush Administration has moved more quickly than any administration since World War II to make government activities, documents and other information secret").

60. Memorandum from John Ashcroft, Attorney General, to Heads of all Federal Departments and Agencies re: The Freedom of Information Act (Oct. 12, 2001) [hereinafter Ashcroft Memorandum], *available at* http://www.usdoj.gov/04foia/ 011012.htm (on file with the American University Law Review).

61. *Id.* Attorney General Ashcroft directed agencies to make a "full and deliberate consideration of the institutional, commercial, and personal privacy interests" when determining whether to make disclosures under FOIA. *Id.* Critics argue this turns FOIA into a balancing act. *See* Schoenhard, *supra* note 1, at 504 (arguing that the Ashcroft Memorandum, in establishing the "concepts of Government transparency and freedom as mutually exclusive goals" of the DOJ, made FOIA "more of a balancing act than a statutory mandate").

62. Ashcroft Memorandum, *supra* note 60 (emphasis added). "The result appears to be that the DOJ will support an agency withholding information from the public unless (a) there is no chance the DOJ will win the subsequent lawsuit; or (b) to support the agency in question might disclose other Government information." Schoenhard, *supra* note 1, at 504.

63. *Id.* Justification for this deviation came from the realities of September 11,

This is a higher threshold for disclosure than the Clinton Administration's policy of defending agency decisions to withhold information only where disclosure would likely harm a party protected by the exemptions.

Approximately five months after agencies received the Ashcroft Memorandum, amidst continuing public anger over the September 11, 2001 attacks,[64] White House Chief of Staff Andrew Card issued further FOIA guidance imploring agencies to safeguard government records relating to weapons of mass destruction ("Card Memorandum").[65] The Card Memorandum instructed agencies to review government information "regarding weapons of mass destruction, as well as other information that could be misused to harm the security of our nation and the safety of our people,"[66] and required agencies to report their reviews to the Office of Homeland Security no later than ninety days after March 19, 2002.[67] In response, agencies removed public access to *thousands* of documents.[68]

A supplemental memorandum from Laura L.S. Kimberly, Acting Director of the Information Security Oversight Office, provided guidance on implementation of the Card Memorandum.[69] Not surprisingly, Kimberly gave a broad definition for "sensitive information," defining it as "government information regarding weapons of mass destruction, as well as other information that could be misused to harm the security of our nation or threaten public

---

2001. To buttress this memorandum, the Bush Administration urges agencies to use FOIA exemptions to prevent potential disclosures relating to the nation's critical infrastructure and to protect agency information that could enable a party to unleash further terror on the U.S. Ashcroft Memorandum, *supra* note 60.

64. *See* Mark Tapscott, *Too Many Secrets*, WASH. POST, Nov. 20, 2002, at A25 (connecting the restriction of government disclosures with the al Qaeda September 11, 2001 attacks).

65. Memorandum from Andrew Card, Assistant to the President and Chief of Staff, to Heads of Executive Departments and Agencies re: Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security (Mar. 19, 2002) [hereinafter Card Memorandum], *available at* http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm (on file with the American University Law Review).

66. *Id.*

67. *Id.*

68. Tapscott, *supra* note 64; *see infra* note 143 and accompanying text (detailing specific reports of information removed from government websites).

69. Memorandum from Laura L.S. Kimberly, Acting Director, Information Security Oversight Office, to Departments and Agencies re: Safeguarding Information Regarding Weapons of Mass Destruction and Other Sensitive Records Related to Homeland Security (Mar. 19, 2002) [hereinafter Kimberly Memorandum], *at* http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm (on file with the American University Law Review).

safety."[70] Kimberly elaborated on the protection of classified information under Executive Order 12958[71] ("Classified National Security Information") and information that had been unclassified or declassified.[72] Importantly, Kimberly also directed that the disclosure of sensitive but unclassified information should be "carefully considered, on a case-by-case basis," alongside the "benefits that result from the open and efficient exchange of scientific, technical, and like information."[73]

Finally, Kimberly instructed all agencies that any FOIA request for records containing sensitive information be processed in accordance with the Ashcroft Memorandum—"giving full and careful consideration to all applicable FOIA exemptions."[74] Coupled with the broad new FOIA exemption for the Department of Homeland Security described in the next section, the federal government, under President Bush, has created an environment in which the public could be denied FOIA's full benefits.[75]

III. THE HOMELAND SECURITY ACT OF 2002

A. The Origins of a Department of Homeland Security

Congress and the President created the Department of Homeland Security ("DHS") in response to the September 11, 2001 terrorist attacks.[76] In the hours following the attacks, government employees from all agencies scrambled to provide assistance to the Bush

70. *Id.*

71. *See id.* (providing for the classification of information that would assist in the development or use of weapons of mass destruction for up to twenty-five years, even though there is a standard of declassifying classified information within ten years of its original classification).

72. *See id.* (indicating that if the information never was classified and never was disclosed to the public under proper authority, but could "reasonably be expected to assist in the development or use of weapons of mass destruction, it should be classified in accordance with Executive Order 12958"; if information was classified and then declassified, but was never disclosed to the public "under proper authority," it should likewise be reclassified under Executive Order 12958).

73. *Id.*

74. *Id.*

75. *See* discussion *infra* Part IV (arguing that the Bush Administration's FOIA policy and the Department of Homeland Security's broad FOIA exemption contribute to an overall climate of nondisclosure).

76. Jessica Reaves, *Homeland Security: A Primer*, TIME (ONLINE ED.), Nov. 19, 2002, *at* http://www.time.com/time/nation/article/0,8599,391161,00.html (on file with the American University Law Review). *But see* Homeland Defense Press Briefing, *supra* note 59 (reporting that President Bush directed Vice President Cheney to begin the task of looking at the current structure of the federal government and its capability of addressing terrorist attacks in May 2001).

Administration.[77] When they encountered procedural red tape and communication barriers, some opined that there should be one unified department to combat and respond to future terrorist attacks on U.S. soil.[78] It took a little over a year for that request to evolve into a new Cabinet-level agency.[79]

The Homeland Security Act of 2002 ("HSA")[80] passed the House in July 2002, but disputes over workers' rights,[81] as well as other controversial provisions,[82] impeded passage in the Senate for

77. Reaves, *supra* note 76.

78. *Id.* Indeed, President Bush's initial proposal of a Cabinet-level Department of Homeland Security called for "substantially transforming the current confusing patchwork of government activities into a single department whose primary mission is to protect our homeland." *Id.*

79. President Bush initially established an Office of Homeland Security by Executive Order on October 8, 2001. *See* Press Release, The White House, Executive Order Establishing Office of Homeland Security (Oct. 8, 2001) (establishing the Office of Homeland Security and the Homeland Security Council), *at* http://www.whitehouse.gov/news/releases/2001/10/20011008-2.html. (on file with the American University Law Review). Senators Joseph Lieberman and Arlen Specter subsequently introduced Senate legislation to create a Cabinet-level Department of Homeland Security. *See* Press Release, Senate Committee on Governmental Affairs, Lieberman, Specter Offer Homeland Defense Legislation (Oct. 11, 2001), *at* http://www.senate.gov/ ~gov_affairs/101101homedefpress.htm (arguing that the country needs an executive-level department to carry out the functions of homeland defense) (on file with the American University Law Review). The idea for a Cabinet-level department was based largely on the recommendations of the U.S. Commission on National Security/21st Century, commonly known as the Hart-Rudman Commission. *Id. See also Critical Infrastructure Protection: Who's In Charge?: Hearing of the S. Governmental Affairs Comm.*, 107th Cong. (2001) (statement of Sen. Cleland, Member, S. Governmental Affairs Comm.) [hereinafter Statement of Cleland] (describing the Commission's finding that it was inevitable a terrorist attack would occur, it was just a matter of when and recommending a "full-blown" homeland defense agency). After President Bush officially supported the creation of a Department of Homeland Security in early June 2002, see Homeland Defense Press Briefing, *supra* note 59 (supporting the creation of a Department of Homeland Security), it was only a matter of time before the Homeland Security Act of 2002 ("HSA") passed in the House and Senate.

80. H.R. 5005, 107th Cong. (2002), Pub. L. No. 107-296, 116 Stat. 2135 (2002).

81. While most Democrats argued that DHS employees should be given the same protections as other government employees, President Bush and other Republicans responded that the President "should have the power to hire, fire, and discipline any staff member for any reason" because "the sensitivity of this department's mission demand[s] fast action." Reaves, *supra* note 76. This debate continued in the Senate for months, until the widespread Republican gains in the midterm elections brought both parties to the "bargaining table" and paved the way for the HSA's ultimate passage. *Id.*

82. Provisions allowing guns in the cockpit, as well as small pox vaccinations, are included in the final Act. *Compromise Reached on Homeland Security Bill*, CNN, Nov. 13, 2002 [hereinafter *Compromise*], *at* http://www.cnn.com/2002/ALLPOLITICS/ 11/12/homeland.security/index.html (on file with the American University Law Review); *see* Reaves, *supra* note 76 (describing the debate over a "Total Information Awareness" system, which would give the government "virtually unfettered access to private information exchanged between U.S. citizens," including e-mail, banking records and travel documents).

months.[83] After Republicans gained seats in the November 2002 midterm elections, the HSA became President Bush's main priority and quickly moved through both houses of Congress, reflecting the President's "dramatically enhanced clout."[84]

The newly-created DHS marks the first major government restructuring since the creation of the Department of Energy in 1977,[85] and the creation of the nation's third largest federal agency.[86] With a beginning budget of $37 billion, DHS encompasses 170,000 workers from twenty-two agencies, including the Secret Service, Border Patrol, Coast Guard, and Customs Service.[87] The Department's mission to coordinate counter-terrorism measures and preemptive defense will be carried out through the Department's four divisions: border and transportation security; emergency preparedness and response; countermeasures for chemical, biological, radiological, and nuclear attacks; and an intelligence clearinghouse.[88]

Buried deep within the HSA, however, is a troubling FOIA development.[89] Despite the DHS's noble duty of protecting national

---

83. *See* Darren Samuelsohn, *Homeland Security Bill Passes Senate With New FOIA Exemptions Included*, GREENWIRE, Nov. 20, 2002, *available at* Westlaw, 11/20/02 EEP-GRW art. 6 (reporting that the new FOIA exemption "that gives U.S. industries, including chemical manufacturers and utilities, an exemption from the [FOIA]" did not gain the same degree of attention from Congress as did numerous other homeland security issues).

84. Helen Dewar, *Homeland Bill Gets Boost*, WASH. POST, Nov. 13, 2002, at A01. In light of the midterm elections in November 2002, President Bush designated passage of the HSA as his main priority for the rest of the Congressional term. *Id.* *See* Helen Dewar, *Homeland Security Legislation Becomes Republican Priority*, WASH. POST, Nov. 9, 2002, at A05 (reporting that House and Senate Republican leaders told President Bush they would spend the post-election session attempting to pass the DHS legislation); *see also Compromise*, *supra* note 82 (citing passage of the Homeland Security Act as "the president's top priority in the lame-duck Congress"). The HSA passed the House by a vote of 299-121, and it passed the Senate by a vote of 90-9. Samuelsohn, *supra* note 83.

85. Reaves, *supra* note 76.

86. GENERAL ACCOUNTING OFFICE, MAJOR MANAGEMENT CHALLENGES AND PROGRAM RISKS: DEPARTMENT OF HOMELAND SECURITY 3 (2003) [hereinafter GAO DHS], *at* http://www.gao.gov/pas/2003/d03102.pdf (on file with the American University Law Review).

87. *Compromise*, *supra* note 82. DHS must quickly and effectively integrate disparate agencies and activities into one cohesive organization, marking a government restructuring of unmatched proportions. GAO DHS, *supra* note 86, at 6.

88. Reaves, *supra* note 76.

89. *See* 148 CONG. REC. S11405-03, S11423 (daily ed. Nov. 19, 2002) (statement of Sen. Leahy) [hereinafter Statement of Leahy] (arguing that the Homeland Security Act of 2002's FOIA provisions are "entirely unnecessary" to the establishment of the Department of Homeland Security). Senator Leahy, the leading FOIA champion in the Senate, deemed the provision "the most severe weakening of [FOIA] in its 36-year history." *Id.* at S11425. Unlike the Ashcroft Memorandum, which implored agencies to be more careful with the release of information, the HSA, through the Critical Infrastructure Information Act of 2002 ("CIIA"), actually provides a blanket

security, its establishing legislation provides a blanket FOIA exemption[90] for private industries supporting the nation's critical infrastructure.[91]

B. A New FOIA Exemption Under the Critical Infrastructure Information Act of 2002

In pertinent part, § 214(a)(1) of the HSA provides:

> 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 . . . *shall be exempt from disclosure under section 552 of title 5, United States Code* (commonly referred to as the Freedom of Information Act).[92]

This provision, subtitled as the "Critical Infrastructure Act of 2002" ("CIIA"), grants authority to impose a fine, up to a year of imprisonment, or both, as well as removal from employment, upon any government offender who discloses this protected infrastructure information.[93] The measure is an exact replica of the FOIA proposal in the original House Act, which passed in July 2002. In the rush to

---

FOIA exemption: the agency cannot release *any* information provided by private industry relating to the nation's critical infrastructure.

That this extreme provision is buried deep in the HSA troubles many. *See, e.g.*, Samuelsohn, *supra* note 83 (quoting Charles Davis, executive director of the Freedom of Information Center at the University of Missouri School of Journalism as stating that "by burying [the FOIA provision] in homeland security, it becomes motherhood and apple pie"); *Administrative Law, Adjudicatory Issues, and Privacy Ramifications of Creating a Department of Homeland Security: Hearing Before the Subcomm. on Commercial & Admin. Law of the House Comm. on the Judiciary*, 107th Cong. 28 (2002) (statement of Peter Swire, Professor of Law, Ohio State University) (citing as troubling the "apparently slipshod manner in which such an important topic was inserted" into the HSA) [hereinafter Statement of Swire].

90. *See* Samuelsohn, *supra* note 83 (quoting an aide to Senator Leahy as stating that the new FOIA exemptions permit the "federal government to trump any state's own FOIA protections." The aide called the FOIA exemption under the Homeland Security Act of 2002 "about as blanket a pre-emption as you can get").

91. The HSA defines "critical infrastructure" as the "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Homeland Security Act of 2002, H.R. 5005, 107th Cong. § 2(4) (2002). This is the same definition Congress used in the USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001). Such a broad definition means that this exemption could apply broadly across many sectors, including the financial services and telecommunications sectors.

92. Homeland Security Act of 2002, H.R. 5005, 107th Cong. § 214(a)(1) (2002) (emphasis added).

93. *Id.* § 214(f); *see* Rena Steinzor, *"Democracies Die Behind Closed Doors": The Homeland Security Act and Corporate Accountability*, 12 KAN. J.L. & PUB. POL'Y 641, 648 (2003) (arguing that this prohibition against disclosure "gilds the lily of confidentiality").

final passage in November, the Senate accepted the prior House version of the legislation.[94]

Implementation of the CIIA FOIA provision came one step closer to fruition with the DHS's issuance of interim final rules, effective January 27, 2003.[95] The rules implement Executive Order 12958 (protecting "Classified National Security Information")[96] which constitutes FOIA Exemption 1, and delineate the Department's general FOIA policy.[97] Moreover, on April 15, 2003, DHS released a proposed rule governing procedures for handling critical infrastructure information under the new CIIA exemption.[98] The proposed rule outlines procedures for the receipt and safeguarding of critical infrastructure information and elaborates on the permissible and prohibited disclosure of this information as provided by the CIIA.[99]

The CIIA FOIA provision will shield from public view sensitive infrastructure data submitted voluntary to federal officials by critical infrastructure owners and operators.[100] Our nation's critical infrastructure traditionally consists of sectors such as information and communications, banking and finance,[101] transportation, and

94. *See Compromise*, *supra* note 82 (describing a compromise on labor rights that allowed for rapid passage of the HSA); *see also* Samuelsohn, *supra* note 83 (reporting that the last homeland security battle "steered clear" of FOIA).

95. According to Homeland Security Secretary Tom Ridge, the interim rule will be issued without a delayed effective date because "notice and public procedure [would be] impracticable, unnecessary, and contrary to the public interest." Freedom of Information Act and Privacy Act Procedures for the Department of Homeland Security, 68 Fed. Reg. 4056 (Jan. 27, 2003) (to be codified at 6 C.F.R. ch. 1 & pt. 5).

96. Classified National Security Information for the Department of Homeland Security, 68 Fed. Reg. 4073 (Jan. 27, 2003) (to be codified at 6 C.F.R. pt. 7).

97. Freedom of Information Act and Privacy Act Procedures for the Department of Homeland Security, 68 Fed. Reg. at 4056-63.

98. Procedures for Handling Critical Infrastructure Information; Proposed Rule, 68 Fed. Reg. 18,524 (Apr. 15, 2003) (to be codified at 6 C.F.R. pt. 29).

99. *See id.* at 18,528-18,529.

100. *See* Christopher J. Dorobek, *Industry Still Leery About FOIA Rules*, FED. COMPUTER WEEK, July 29, 2002, at 12. Moreover, the provision will exempt submitters from civil or antitrust liability and impose criminal penalties on government employees who disclose the designated information. *See* Statement of Leahy, *supra* note 89, at S11425 (asserting that "[c]riminalizing disclosures . . . is an effective way to quash discussion and debate over many aspects of the Government's work").

101. A June 2002 survey by Business Software Alliance, a technology industry association, showed that seventy-four percent of surveyed technology professionals felt "nearly certain" that a cyber attack would be launched against American financial institutions by June 2003. William Matthews, *Rep. Smith Sounds Cyberalarm*, FED. COMPUTER WEEK, July 29, 2002, at 12; *see also* Thomas P. Vartanian, *September 11 Attacks Illustrated New Risks to Banking System*, 167 AM. BANKER, Nov. 2, 2001 (citing an increasing number of attacks on financial systems and arguing that increased computer access to these systems could mean that these attacks are likely to continue). Of particular concern to Vartanian is that "[c]ritical security

energy.[102] Government officials argue that this measure will facilitate public-private information sharing and will give the government a toehold into the private sector so that it may respond quickly and effectively to any attack on the nation's critical infrastructure.[103] Among the information covered by the provision are data concerning "any planned or past assessment, projection, or estimate of the security vulnerability of a protected system or critical infrastructure . . . any planned or past operational problem or solution . . . related to the security of a protected system or critical infrastructure; or any threat to the security of a protected system or critical infrastructure."[104]

The CIIA FOIA provision shields from liability critical infrastructure owners and operators who "voluntarily" report information regarding vulnerabilities.[105] Importantly, some courts

---

infrastructure and data protection issues arise when a company's electronic networks and databases are compromised"; in the case of banks, information containing "proprietary business information, monetary value, intellectual property, or customer information" could be compromised or stolen. *Id.* Ultimately this could also lead to adverse public relations if such an attack were to be disclosed to the public. *Id.*

For an assessment of how the events of September 11, 2001 have affected the financial services industry, *see id.* (arguing that a "distinct shift" has occurred in the financial services industry for several reasons, such as the likelihood of customer records being more accessible to government officials and the need to reevaluate risk exposure in the flow of money and information in the banking and payment systems post-September 11, 2001).

102. MARK S. SAWYER, NAT'L SEC. AGENCY, HOMELAND SECURITY ORGANIZATIONS, MISSIONS, RESPONSIBILITIES, AND STRATEGIES 24 (2002) (on file with the American University Law Review). Other critical infrastructure sectors include water supply, emergency law enforcement services, emergency fire service and continuity of government services, and public health services. *Id.*

103. John Tritak, director of the Commerce Department's Critical Infrastructure Assurance Office, argues that the real goal of the DHS legislation was to "create an environment where dynamic information sharing is taking place and problems can be dealt with in real time." Brian Krebs, *Critics Blast IT Loophole in Homeland Security Plan*, WASH. POST, July 24, 2002, *at* http://www.washingtonpost.com/ac2/wp-dyn/A58311-2002Jul24 (on file with the American University Law Review); *see also* 148 CONG. REC. S11562-03 (daily ed. Nov. 19, 2002) (statement of Sen. Bennett) [hereinafter Statement of Bennett] (arguing that because the private and public sectors are increasingly interconnected and are terrorist targets, it makes sense for both targets to share information with each other). *See generally* discussion *infra* Part IV.C (listing the government's reasons for wanting to facilitate public-private information sharing relationships).

104. *See* Summerill, *supra* note 37, at 25, 26 (citing S. 1456 § 4(3) and noting that industry views this type of information as proprietary data).

105. Industry seems pleased with this new blanket exemption. *See, e.g.*, Darren Samuelsohn, *Senate in Home Stretch on Cabinet-level Bill with FOIA Exemption*, ENV'T & ENERGY DAILY, Nov. 18, 2002 (quoting Kate McGloon, a spokeswoman for the American Chemistry Council, as stating that the new language is a "step in the right direction" because it will give industry the assurance it needs to provide the government with critical security data without fear that the information would be released to the public and serve as a guidepost for future terrorist attacks), *available at* Westlaw, 11/13/02 EEP-EED art. 2; *Industry Exemption in Homeland Security Bill Sparks Controversy*, OIL DAILY, Nov. 18, 2002, *available at* 2002 WL 101846383

distinguish between information submitted voluntarily to the government, and information required to be submitted to the government.[106] When the government seeks voluntary disclosure of business information, the government must keep that information confidential "if it is of a kind that would customarily not be released to the public by the person from whom it was obtained."[107] However, if the government requires private entities to disclose information, that information must be kept confidential only if its disclosure is likely to (1) impair the government's ability to obtain necessary information in the future, or (2) "cause substantial harm to the competitive position" of the entity from whom the government obtained the information.[108]

Prior to the HSA's final passage, Senators Leahy, Bennett and Levin reached a compromise that proposed to narrow the broad CIIA FOIA provision but still provide additional nondisclosure protections for certain sensitive records.[109] The key difference between the final version of the CIIA FOIA provision and the compromise provision is that the compromise merely provided a FOIA exemption for "records," whereas the final version protects the broader category of "information."[110] The Senators recognized that the "information" standard is vague and could be exploited simply by reference to private sector information contained in a government record.[111] Moreover, the compromise would have limited the exemption to records pertaining to "the *vulnerability of and threats to* critical infrastructure," rather than the CIIA's broader language requiring

(reporting that the American Petroleum Institute "believes that making public security-sensitive information is a potential threat to refineries, pipelines, and offshore facilities," and thus supports the new FOIA exemption).

106. *See* Backes, *supra* note 38, at 978 (citing McDonnell Douglas Corp. v. Nat'l Aeronautics & Space Admin., 895 F. Supp. 319, 326 (D.D.C. 1995), Critical Mass Energy Project v. Nuclear Regulatory Comm'n, 975 F.2d 871, 879 (D.C. Cir. 1992) (en banc), and Westinghouse Elec. Corp. Research & Dev. Ctr. v. Brown, 443 F. Supp. 1225, 1228 (E.D. Va. 1977)).

107. *See* Backes, *supra* note 38, at 978 (citing *Critical Mass*, 975 F.2d at 879).

108. *See id.* (citing *Westinghouse*, 443 F. Supp. at 1228-29).

109. This compromise was offered and approved unanimously during the Senate Governmental Affairs Committee markup on the bill. *Amendment to Scale Back FOIA Exemption for Homeland Security Department* (July 25, 2002) [hereinafter *Amendment*], *at* http://www.fas.org/sgp/news/2002/07/leahy-foi.html (on file with the American University Law Review). *See* Statement of Leahy, *supra* note 89 at S11425 (asserting that the enacted version "jettisoned the bipartisan compromise" and "replaced it with a big-business wish-list gussied up in security garb").

110. *See* Statement of Leahy, *supra* note 89, at S11425 (arguing that by using the term "records" rather than "information," the government would avoid the "adverse result of government agency-created and generated documents and databases being put off-limits . . . simply if private sector 'information' is incorporated").

111. *Amendment*, *supra* note 109.

protection of *any* "critical infrastructure information."[112] After all, under the CIIA, *any* document labeled as containing "critical infrastructure information" would be off-limits to the public.

Following FOIA legal precedent,[113] the compromise legislation also ensured that those portions of records that do not fall within a specific FOIA exemption would still be disclosed to FOIA requesters.[114] Finally, the compromise legislation did not exempt industry from civil or antitrust liability, did not preempt state and local freedom of information laws, and only applied to records submitted to DHS.[115] This compromise was all but ignored in November 2002, perhaps due to the Republicans' enhanced clout following the November midterm elections.[116] Though they differed in their respective approaches, both the CIIA FOIA provision and the Senate compromise provision focused on critical infrastructure protection because our nation's physical and cyber infrastructure is a potential target for future terrorist attacks.

1. Critical infrastructure protection

Just as the U.S. economy was a target on September 11, 2001,[117] it is a foregone conclusion that terrorists will continue to target our nation's critical infrastructure.[118] This places the U.S. government in a precarious position, as estimates indicate that up to ninety percent

112. *Id.* (emphasis added).

113. *See generally* Envtl. Prot. Agency v. Mink, 410 U.S. 73 (1973) (holding that agencies may disclose nonsecret factual portions of protected records).

114. Statement of Leahy, *supra* note 89.

115. *Amendment*, *supra* note 109.

116. *See* Eleanor Clift, *Capitol Letter: The Latest Debacle*, NEWSWEEK, Nov. 22, 2002 (arguing that the Bush Administration used its "post-election muscle . . . to extend a blanket of secrecy over government business that has even a tangential link to homeland security"), *available at* http://stacks.msnbc.com/news/838892.asp (on file with the American University Law Review). Clift argues that the DHS FOIA provision passed "with nobody paying attention and the Democrats demoralized." *Id.*

117. *See* Ross Kerber, *Send in the Cyber G-Men: Private Sector Urged to Partner in Defense*, BOSTON GLOBE, Oct. 15, 2001, at C1 (citing a report by Dartmouth's Institute for Security Technology Studies as stating that the September 11, 2001 attacks closed financial markets and "destroyed a significant component of the financial information infrastructure in New York City"); *see also Critical Infrastructure Protection: Who's in Charge?: Hearing of the S. Governmental Affairs Comm.*, 107th Cong. 4 (2001) (statement of Sen. Carnahan, Member, S. Governmental Affairs Comm.) (asserting that the September 11, 2001 terrorists not only wanted to bring down our buildings, but to injure our economy, our military, and our "financial and political infrastructure").

118. Basically, the definition of "infrastructure covers just about everything of value in our country." *See* Statement of Cleland, *supra* note 79 (noting that "[n]othing affects Americans more than the disruption of the Nation's [infrastructure]"). Our nation's infrastructure sectors are increasingly becoming interdependent, so disruptions in one sector could ultimately have repercussions across many sectors. *Id.*

of the nation's critical infrastructure industries are privately owned and independently operated,[119] and many of them remain vulnerable to attack.[120] Many government insiders believe that the new CIIA FOIA exemption will encourage these industries to share sensitive information with the government and ultimately lead to public-private cooperation in the "war against terrorism."[121] However, this Comment will later demonstrate that even with this broad new exemption, critical infrastructure owners and operators might continue to withhold sensitive information due to trust and uncertainty issues surrounding potential partnerships with the government.[122]

2. The likelihood of cyber attacks

The CIIA FOIA provision addresses not only conventional attacks on the nation's physical critical infrastructure, but also unconventional attacks on our nation's computer information and communication infrastructure.[123] Key sectors such as telecommunications, power distribution, water supply, public health services, national defense, and emergency services all depend upon

119. *See* Statement of Davis, *supra* note 9 (emphasizing that although sensitive critical infrastructure information is now shared within some industries, such information is not shared with the government or shared across industries); *see also* Exec. Order. No. 13,231, 3 C.F.R. 806 (2002), *reprinted* in 6 U.S.C. § 121 (2002) (implementing a critical infrastructure protection program composed of a "voluntary public-private partnership, involving corporate and nongovernmental organizations.").

120. *See* Council on Foreign Relations, *supra* note 7, at 26 (reporting that much of our critical infrastructure is as vulnerable to attack today as it was a year ago); *see also Critical Infrastructure Protection: Who's In Charge?: Hearing of the S. Governmental Affairs Comm.*, 107th Cong. 28 (2001) (statement of Frank Cilluffo, Senior Policy Analyst and Deputy Director, Center for Strategic and International Studies) [hereinafter Statement of Cilluffo] (arguing that the nation's infrastructure is a "popular terrorist target" and that the "destruction or incapacitation [of these systems] could have a debilitating effect on U.S. national or economic security").

121. *See* NSPPCIKA, *supra* note 6, at 26 (reporting that the CIIA assists in removing legal obstacles to public-private information sharing).

122. *See* discussion *infra* Part IV.C.3 (discussing cultural problems such as industry distrust and uncertainty as obstacles to public-private information sharing).

123. This has significant import because "[c]omputers power the economy." *See* Emily Frye, *The Tragedy of the Cybercommons: Overcoming Fundamental Vulnerabilities to Critical Infrastructures in a Networked World*, 58 BUS. LAW. 349, 350 (2002) (quoting National Security Advisor Condoleeza Rice as stating that "the cyber economy is the economy" in her Address to the Partnership for Critical Infrastructure of the U.S. Chamber of Commerce (Mar. 23, 2001)), *available at* http://www.house.gov/jec/security.pdf) (on file with the American University Law Review). *See generally* Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207 (2002) (arguing that cyber attacks targeting the nation's critical infrastructure are an act of aggression and allow the victim state to act in anticipatory self-defense).

networked operations.[124] Experts warn that our population's increased reliance on computer networks[125] could ultimately pose a new threat of cyber attacks.[126] Frighteningly, just *one* successful cyber attack has the potential to cause widespread damage and result in thousands of deaths.[127] As enumerated by counter-terrorism adviser

---

124. Tim Hackman, director of public affairs for International Business Machines Corp.'s government programs, argued that "[c]yber-security and electronic infrastructure are such a pervasive foundation of everything in our country that we need to raise the focus of that in the [DHS] legislation." Ariana Eunjung Cha, *Cyber-Security is Underplayed, Industry Says*, WASH. POST, July 4, 2002, at E01.

125. *See Creating the Department of Homeland Security: Consideration of the Administration's Proposal Hearings Before the Subcommittee on Oversight & Investigation of the House Comm. on Energy & Commerce*, 107th Cong. 335 (2002) (statement of Robert F. Dacey, Director, GAO) [hereinafter Statement of Dacey] (arguing that "widespread interconnectivity poses significant risks to our computer systems and . . . the critical operations and infrastructures they support"); *see also* Statement of Bennett, *supra* note 103 (stating that pipelines can be controlled remotely by computers, and that a weakness in a telecommunications system could affect both the functioning of the military and the financial services sector).

126. Richard Clarke, former National Coordinator for Security Infrastructure Protection and Counterterrorism within the National Security Counsel and currently President Bush's special advisor on cyberspace security, cautioned that terrorists could attack the U.S. through cyber attacks, consisting of attacks on the nation's infrastructure "not from bombs but with computers." *See* Jensen, *supra* note 123, at 211 (quoting Richard Clarke, Keynote Address: *Threats to U.S. National Security: Proposed Partnership Initiatives Toward Preventing Cyber Terrorist Attacks*, 12 DEPAUL BUS. L.J. 33, 35 (1999)). Clark posed the frightening prospect that the U.S. may experience an "electronic Pearl Harbor," when concurrent cyber attacks could disable cities' power, telecommunications, and transportation. *Id.* at 212 (quoting Clarke, *supra*, at 38). *See also* Kerber, *supra* note 117 (reporting that security planners have noted that past military actions "prompted a response from hackers worldwide").

127. *See* Matthews, *supra* note 101, at 12 (reporting the remarks of Rep. Lamar Smith to a group of technology industry insiders and congressional staffers). As an example of just how vulnerable our computer networks may be, see Jensen, *supra* note 123, at 209, in which the author describes an October 2000 computer hack at the Microsoft Corporation. The hackers may have accessed Microsoft's software source code using a relatively unsophisticated program (called a Trojan horse), giving them the ability to either alter program operations or install hacker tools into the software. *Id.* at 210 (citing ARNAUD DE BORCHGRAVE ET AL., CENTER FOR STRATEGIC & INTERNATIONAL STUDIES, CYBER THREATS AND INFORMATION SECURITY MEETING THE 21ST CENTURY CHALLENGE iv (2000), *available at* http://www.csis.org/homeland/reports/cyberthreatsandinfosec.pdf) (on file with the American University Law Review). Although Microsoft denied any serious damage, *see id.* at 209 (citing Dan Verton, *Think Tank Warns That Microsoft Hack Could Pose National Security Risk*, COMPUTERWORLD, Dec. 2000, *available at* http://www.computerworld.com/security topics/security/story/0,10801,55656,00.html) (on file with the American University Law Review), a report by the Center for Strategic and International Studies ("CSIS") argued that "if this could happen to Microsoft, then no company is safe." *See id.* (citing BORCHGRAVE ET AL., *supra*). The CSIS report further argued that if someone can hack into the "heart of the ubiquitous Windows program [they] can hack into any PC in the world that uses it and is connected to the Internet." Jensen, *supra* note 123, at 210 (citing BORCHGRAVE ET AL., *supra*, at iv). Some notorious hacking cases remain unsolved. *See* Kerber, *supra* note 117 (citing attacks that shut down Yahoo Inc. and E*Trade in February 2000). Criminals continue to take advantage of weaknesses in computer networks. Recently, Federal authorities charged three men in the largest identity theft case to date, in which the perpetrators allegedly obtained

James Kallstrom at a House hearing, the potential cyber attack scenarios are frightening: air traffic control equipment malfunctions, heating, ventilation, and air conditioning systems modified to circulate harmful gases within a large office complex, 911 telephone communications interrupted, electrical blackouts, power dam water flow modified to allow downstream flooding, and financial market disruption.[128] Through use of the Internet, cyber terrorists could carry out all of these attacks at once.[129]

Indeed, terrorists may soon use the Internet as a "direct instrument of bloodshed."[130] Thus far, no traditional terrorist groups have used the Internet to attack our critical infrastructure.[131] However, evidence indicates that members of al Qaeda have researched the possibility of electronically disabling or destroying our nation's critical infrastructure, including dams and communications systems.[132] In a

---

network access codes to credit reports and defrauded some 30,000 individuals. *Feds Charge 3 in Massive Credit Fraud Scheme*, CNN, Nov. 25, 2002, *at* http://www.cnn.com/2002/LAW/11/25/ID.theft/index.html (on file with the American University Law Review).

The alleged criminals deleted the victims' bank accounts, ordered new checks, ATM cards, and credit cards using the victims' identities, and opened new lines of credit, only to immediately disburse the funds. *Id.*

128. *See* Statement of Kallstrom, *supra* note 10 (arguing that technology can be used as a weapon of mass destruction).

129. *See* Statement of Cilluffo, *supra* note 120, at 27 (stating that "[T]he comparatively low-tech means employed by the terrorists raises the possibility of a cyber strike," or even a combination of physical and virtual attacks on one or more critical infrastructures).

130. *See Creating the Department of Homeland Security: Consideration of the Administration's Proposal Hearings Before the Subcommittee on Oversight & Investigation of the House Comm. on Energy & Commerce*, 107th Cong. 226 (2002) (statement of Guy Copeland, Vice President, Computer Sciences Corporation) [hereinafter Statement of Copeland] (citing evidence of al Qaeda's internet skills and interest in using computers to launch an attack against physical structures).

131. Statement of Dacey, *supra* note 125.

132. *See, e.g.*, *id.* (stating that officials discovered information on computerized water systems in al Qaeda camps in Afghanistan); Jay Lyman, *Worries Mount Over Terrorist Cyber Assault*, NEWSFACTOR NETWORK, June 27, 2002 (realizing that al Qaeda may posses working knowledge of vital infrastructure systems), *available at* http://www.newsfactor.com/perl/story/18426.html (on file with the American University Law Review); *see also* Brett Stohs, *Protecting the Homeland by Exemption: Why the Critical Infrastructure Information Act of 2002 Will Degrade the Freedom of Information Act*, 2002 DUKE L. & TECH. REV. 18 (2002) (noting that "one of the hottest perceived threats to America" is "cyberterror" using our electronic infrastructure). Moreover, key al Qaeda members have shown a high degree of technical proficiency regarding computer systems. Kerber, *supra* note 117. For example, investigators found that Ramzi Yousef, the convicted mastermind of the 1993 World Trade Center bombing, encrypted details of other attack plans on his laptop computer. *Id.* Investigators also discovered an al Qaeda hideout in Pakistan that was used solely for the purpose of training operatives in cyber warfare and hacking. *See also* Frye, *supra* note 123 (citing Kelli Arena & David Ensor, *U.S. Infrastructure Information Found on Al Qaeda Computers* (June 27, 2002), *at* http://www.cnn.com/2002/US/06/27/alqaeda.cyber.threat/index.html (on file with the American University Law Review)).

briefing for members of Congress on July 23, 2002, Representative Lamar Smith warned that there is a fifty percent chance that the next al Qaeda terrorist strike against the U.S. will somehow involve a cyber attack.[133] Therefore, determining how to secure cyberspace is critical to our national security, especially considering this country's dependence on computer networks.[134]

The federal government used the U.S.'s apparent vulnerabilities in our physical and electronic infrastructure to justify legislation and policies that could undermine FOIA. However, the preexisting FOIA exemption framework provides the government with adequate tools to protect critical infrastructure information, thus obviating the need for this erosion of FOIA.

IV. DISCUSSION: THE UNNECESSARY EROSION OF FOIA AND ITS IMPLICATIONS FOR GOVERNMENTAL TRANSPARENCY, PUBLIC SAFETY AND PUBLIC-PRIVATE INFORMATION SHARING PARTNERSHIPS

A. The Bush Administration's Policy Shift Takes a Broad Step Toward Restricting Public Access to Government Information

As described above, the Ashcroft Memorandum effectively requires the public to have a "need to know" the information it requests,[135] the same legal standard that existed prior to the enactment of FOIA in 1966.[136] Such a high standard of proof on the part of the requesters

133. *See* Matthews, *supra* note 101, at 12. Representative Smith, Chairman of the House Judiciary Committee's Crime, Terrorism, and Homeland Security Subcommittee, warned that there is evidence that al Qaeda operatives have searched U.S. websites and researched the country's electronic infrastructure to find ways to "disable power and water supplies, disrupt phone service and damage other parts of the infrastructure." *Id.* He particularly cautioned that al Qaeda members might attempt to disable California's energy network. *Id.*

134. *See* Cha, *supra* note 124, at E01 (discussing the need for cyber-security provisions in the HSA); *see also* Statement of Davis, *supra* note 9, at H5826 (arguing that the "vulnerabilities to attack on Federal information systems [have] grown exponentially," and that the "high degree of dependence between information systems . . . exposes the Federal Government's computer networks to benign and destructive disruptions").

135. *See* discussion *supra* Part II.C (describing how Attorney General Ashcroft contributed to the Bush Administration's FOIA policy); *see also* Tom Beierle & Ruth Greenspan Bell, *Don't Let 'Right to Know' be a War Casualty*, CHRISTIAN SCI. MONITOR, Dec. 20, 2001, at 9; *see* Parker, *supra* note 3 (quoting Gary Bass, executive director of OMB Watch, as stating that "[w]e seem to be shifting to the public's need to know instead of the public's right to know"). Analysts believe that the Bush Administration's clampdown on government disclosure "stands out in part because it follows a decade in which . . . improving technology [made] government more accessible to Americans." *Id.* One may naturally draw the conclusion that such an environment reinforced the public's "right to know" certain government information.

136. *See* GAO, *supra* note 22, at 4 (explaining how the enactment of FOIA, with its

could give agencies a green light to restrict access to government information—a result that could ultimately diminish the American public's legal right of free and open access to government information.[137]

Further, Attorney General Ashcroft guarantees that DOJ will defend agency actions so long as it finds a "sound legal basis" for the agency's reasoning.[138] In turn, this could overwhelm the federal court system if the public feels it has not been afforded an appropriate administrative remedy.[139] DOJ officials argue that Attorney General Reno's FOIA memorandum "raised the bar for FOIA refusals," and that Attorney General Ashcroft's FOIA memorandum simply reverts to the standard that had existed prior to the Clinton Administration.[140] Regardless, this new standard for litigating FOIA cases in light of heightened threats to national security could indicate that the DOJ is "less committed to open government" post-September 11, 2001.[141]

"right to know" standard, supplanted the previous "need to know" basis governing access to government information).

137. *See* Summerill, *supra* note 37, at 28 (arguing that "[c]itizens of a democratic society deserve disclosure of government records to ensure government accountability"); *see also* Gidiere & Forrester, *supra* note 2, at 141 (arguing that the Ashcroft Memo's "'sound legal basis' standard is much more slanted toward withholding" government records from FOIA disclosure than the Reno Memo's "foreseeable harm" standard).

138. Ashcroft Memorandum, *supra* note 60.

139. *See* Vanessa Blum, *Administration Won One FOIA Fight, But Battle is Far From Over*, THE RECORDER, Dec. 16, 2002 (reporting on FOIA challenges in our nation's courtrooms and quoting Natural Resources Defense Council general counsel Sharon Buccino as saying that "the White House is not off the hook" when it comes to FOIA disclosures). Another industry insider, Georgetown University Law Center professor and former litigation director of Public Citizen, David Vladeck, commented that DOJ was ordered by the White House "to litigate these cases aggressively" and that the new battle for information in the courtrooms is "absolute trench warfare." *Id.*

140. *Id.* (reporting a joke by David Sobel, general counsel of the Electronic Privacy Information Center, that "even under Reno, he never had a case in which the Justice Department refused to represent an agency"). *But see* James V. Grimaldi, *At Justice, Freedom Not to Release Information*, WASH. POST, Dec. 2, 2002, at E01 (arguing that "[i]t is not that the Reno Justice Department was particularly enamored with FOIA. But at least attorneys didn't have carte blanche to disregard the law.").

141. *See* Rotenberg, *supra* note 9, at 1124 (citing Beierle & Bell, *supra* note 135, at 9; *On the Public's Right to Know: The Day Ashcroft Censored Freedom of Information*, S.F. CHRON., Jan. 6, 2002, at D4; *Ashcroft sends chilling message to FOIA: Memo urging caution over freedom of information requests needs to be reviewed*, VENTURA CITY STAR, Jan. 11, 2002, at B6; and Helen Thomas, *President Bush and John Ashcroft Trample the Bill of Rights*, SEATTLE POST-INTELLIGENCER, Nov. 16, 2001, at B6); *see also Department of Justice Oversight: Preserving our Freedoms While Defending Against Terrorism, Hearing Before the S. Comm. on the Judiciary*, 107th Cong. 310-14 (2001) (statement of John Ashcroft, U.S. Attorney General) (outlining the Bush Administration's tactics in fighting terrorism and defending the Administration's decision to keep confidential information that might impede the government's national security efforts), *available at* http://www.usdoj.gov/ag/testimony/2001/1206transcriptsenatejudiciarycommittee.htm (on file with the American University Law Review); Beierle & Bell, *supra* note

The Bush Administration memoranda encouraged the protection of sensitive information through use of FOIA's statutory exemptions.[142] Although the ultimate result of the Ashcroft and Card memoranda appears to be a reduction in the amount of government information available to the public,[143] the memoranda are important because they suggested ways to work within FOIA's preexisting statutory framework, using Exemptions 2[144] and 4[145] to protect sensitive information.[146] Despite efforts to encourage the protection of sensitive information using this framework, private industry remains reluctant to share sensitive information with the government. Many critical infrastructure owners and operators believe the preexisting FOIA exemptions do not provide adequate disclosure protections and could open industry to potential liability.

135, at 9 (asserting that the presumption in the Bush Administration is that information is inherently risky).

142. *See* Kimberly Memorandum, *supra* note 69 (instructing agencies to protect sensitive critical infrastructure information under Exemption 2 (5 U.S.C. § 552(b)(2)), and to protect private sector information voluntarily submitted to the Government under Exemption 4 (5 U.S.C. § 552(b)(4))).

143. *See* Tapscott, *supra* note 64 (reporting that the Pentagon removed approximately 6,000 Department of Defense documents from disclosure in compliance with the Card Memorandum, and lamenting that now no one "outside of government can verify that any of those documents contained information that could help terrorists"); *see also* PEW INTERNET & AMERICAN LIFE PROJECT, ONE YEAR LATER: SEPTEMBER 11 AND THE INTERNET 8, 9 (2002) (providing an extensive listing of website information to which government agencies prevented access post-September 11, 2001, including the removal of information relating to nuclear facilities from the Department of Energy website, the removal of a security report for chemical plants from the Agency for Toxic Substances and Disease Registry website, and the denial of access to the National Pipeline Mapping System on the Department of Transportation website), *available at* http://www.pewinternet.org/reports/pdfs/PIP_9-11_Report.pdf (on file with the American University Law Review). The Pew study reported that the Card and Ashcroft memoranda resulted in the removal of documents from government websites, as well as terminating certain websites in their entirety. *Id.* The Department of Energy completely removed the website for the National Transportation of Radioactive Materials from the Internet. *Id.* at 9. A Pew survey from June 26, 2002, to July 26, 2002, found that only twenty-five percent of the public was aware that the government had sealed off access to some of its sensitive websites. *Id.*

144. 5 U.S.C. § 552(b)(2) (2002) (exempting "internal personnel rules and practices of an agency").

145. *Id.* § 552(b)(4) (exempting "trade secrets and commercial or financial information obtained from a person and privileged or confidential").

146. Similarly, the White House's *National Strategy for Homeland Security* also provides a framework for working within the preexisting exemption framework to address national security concerns. *See* NSHS, *supra* note 10, at 56 (citing FOIA's exemption framework as protecting sensitive information when its disclosure could harm the public interest or frustrate national security efforts). The document advocates "narrowly limiting public disclosure" of sensitive information so as not to compromise principles of transparency and government accountability. *Id.* at 48.

B. Private Industry is Reluctant to Enter Into Public-Private Information Sharing Partnerships Without Protections to Ensure the Integrity of its Sensitive Business Data

Private industry faces a significant challenge in protecting its assets from attack.[147] The government neither owns nor operates the majority of the nation's critical infrastructure. As a result, private industry must provide the first line of defense to protect its own systems.[148] This entails increased investments in security spending.[149] Complicating this task, industry is also in the midst of coping with the consequences of an economic downturn.[150] Some critical infrastructure owners and operators are now forced to focus on remaining in business. Protecting their companies from potential terrorist attacks may be a secondary priority.[151]

While private industry struggles to stay in business, the government seeks cooperation to fortify protection of the nation's critical infrastructures.[152] Industry could benefit from this interaction: in exchange for providing information to the government concerning infrastructure vulnerabilities, the government could provide industry with advice in making security investment decisions, assistance if the "threat at hand exceeds [industry's] capability to protect itself," and "timely warning" and assurances that the government would focus on the protection of those infrastructures that face a "specific, imminent threat."[153]

---

147. *See generally* NSPPCIKA, *supra* note 6 (describing the financing and high degree of effort industry must put forth in order to protect its infrastructures).

148. *Id.* In many cases, private firms possess better technical expertise and more adequate means to protect "the infrastructure they control" than the government. NSHS, *supra* note 10, at 33. Still, industry faces many challenges in this new threat environment. *See* NSPPCIKA, *supra* note 6, at 8 (arguing that although critical infrastructure owners and operators have always been responsible for protecting their systems, this framework was not designed to cope with significant terrorist threats or the ensuing economic or psychological fallout).

149. *Id.* at 20.

150. *Id.* at 22.

151. *Id.* Supporting this assertion, the Brookings Institution argues that private markets do not adequately protect against terrorist attacks because businesspersons tend to focus more on the pursuit of profit than the possibility that their facilities could come under attack. THE BROOKINGS INSTITUTION, PROTECTING THE AMERICAN HOMELAND: ONE YEAR ON 80-82 (2003).

152. *See* THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE, THE NSTAC'S RESPONSE TO THE NATIONAL PLAN (2001) [hereinafter NSTAC RESPONSE] (reporting that while the government focuses on shoring up national security, private infrastructure owners and operators focus more on "common business imperatives"), *available at* http://www.ncs.gov/NSTAC/National PlanReport-Final.htm (on file with the American University Law Review).

153. NSPPCIKA, *supra* note 6, at xi.

Despite these potential benefits, industry is still reluctant to share sensitive business information with the government due to concerns that FOIA requests could lead to public disclosure of those communications, opening up the possibility of antitrust and other potential liability.[154] Overall, private industry articulates two major concerns about communicating vulnerabilities to the federal government: first, a risk that this information would become public through the country's disclosure laws, resulting in a loss of proprietary information and an increased liability, and second, the potential for antitrust and other legal action against cooperating companies.[155]

Industry insiders argue that "information sharing is a risky proposition with less than clear benefits."[156] Purported uncertainty about current disclosure laws leads companies to avoid the potential risk that such sensitive information could ultimately become public through FOIA and similar state statutes.[157] Industry groups thus

154. *See* NSHS, *supra* note 10, at 33. *See generally* GENERAL ACCOUNTING OFFICE, INFORMATION SHARING: PRACTICES THAT CAN BENEFIT CRITICAL INFRASTRUCTURE PROTECTION 7 (2001) [hereinafter GAO IS] (detailing industry's concerns that release of this type of sensitive information could have damaging effects including lowering customer confidence and providing advantages to competitors).

155. *See* Frye, *supra* note 123, at 361 (reporting that at least two major industry organizations, the Information Technology Association of America and the Partnership for Critical Infrastructure Security, have raised these concerns). John Tritak, Director of the Critical Infrastructure Assurance Office within the U.S. Department of Commerce, testified that industry has long voiced these concerns, and that industry's uncertainty regarding FOIA's legal framework is a "key impediment" to information sharing. *Securing Our Infrastructure: Private/Public Information Sharing: Hearing Before the S. Comm. on Governmental Affairs*, 107th Cong. 79 (2002) (statement of John S. Tritak, Director, Critical Infrastructure Assurance Office, U.S. Dep't of Commerce) [hereinafter Statement of Tritak].

156. *See Securing Our Infrastructure: Private/Public Information Sharing: Hearing Before the S. Comm. on Governmental Affairs*, 107th Cong. 97-98 (2002) (statement of Harris N. Miller, President, Information Technology Association of America) [hereinafter Statement of Miller] (elaborating that no company would want sensitive, and potentially damaging, information to be made public—especially when it could "jeopardize [that company's] market position" and investor confidence); *see also* Dorobek, *supra* note 100, at 12 (discussing industry's continued hesitance regarding FOIA). Stanley Jarocki, Chairman of a Financial Services Information Sharing and Analysis Center and Vice President of Information Technology Security for Morgan Stanley, commented that many companies are wary of the risks of sharing this type of critical information. *Id.* Ronald Dick, director of the Federal Bureau of Investigation's National Infrastructure Protection Center, asserted that industry believes that the law on FOIA exemptions is unclear. *Id.* In contrast, Representative Janice Schakowsky, ranking member of the House Government Reform Committee's Government Efficiency, Financial Management, and Intergovernmental Relations Subcommittee, finds it "shocking" that industry would be reluctant to share information that could prove critical for homeland security. *Id.* Representative Schakowsky argued that Congress should not keep this information secret simply because businesses prefer that result. *Id.*

157. Statement of Miller, *supra* note 156; *see also* Statement of Tritak, *supra* note 155 (arguing that so long as companies perceive the potential for FOIA disclosure of

argue that FOIA disclosures must be restricted to ensure the free flow of information to the government without fear of reprisal or public scrutiny.[158] Industry insiders point to antitrust concerns as another legal obstacle to information sharing, because "[t]he antitrust laws focus on sharing information concerning commercial activities,"[159] which could be implicated by public-private cooperation.

With these concerns in mind, the CIIA FOIA provision responds to the fear that critical infrastructure owners and operators would not comply voluntarily with the government's information requests without new disclosure protections.[160] Moreover, the CIIA FOIA provision addresses industry's other liability concerns by providing for the legal immunity of infrastructure owners and operators who voluntarily provide infrastructure data, and by imposing criminal penalties upon those government officials who disclose this information.[161] Although it remains to be seen whether industry will view these new protections as an incentive to share sensitive information with the government, current FOIA law indicates that the preexisting exemption framework already protects from disclosure this type of critical infrastructure information.

C. The Critical Infrastructure Information Act of 2002 Contains an Overly Broad and Unnecessary FOIA Exemption

Industry's concerns about public disclosure of sensitive information[162] seem credible initially because FOIA is a disclosure

---

sensitive documents, a "common sense risk assessment" leans toward nondisclosure). Scott Charney, Chief Security Strategist for Microsoft Corp., argued that many companies feel the preexisting exemption framework provided "hazy definitions," and could perhaps lead to "endless litigation." Krebs, *supra* note 103. Charney made this argument in support of a broad, concrete FOIA exemption for the DHS. *Id. See generally* THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE, INFORMATION SHARING/CRITICAL INFRASTRUCTURE PROTECTION TASK FORCE REPORT C-1–C-17 (2000) [hereinafter NSTAC TASK FORCE REPORT] (analyzing industry perspectives on FOIA and listing different information sharing initiatives' potential exposure to disclosure laws), *available at* http://www.ncs.gov/NSTAC/NSTACXXIII/Reports/ISCIP-Final.pdf (on file with the American University Law Review).

158. GAO IS, *supra* note 154, at 16; Samuelsohn, *supra* note 105; *see* Statement of Miller, *supra* note 156 (contending that the government unfairly expects private industry to share sensitive information without any "ironclad assurances of confidentiality").

159. Statement of Miller, *supra* note 156; *see* Statement of Tritak, *supra* note 155.

160. Additionally, official government sources, such as the White House's *National Strategy for Homeland Security*, declare that private firms should be assured that "good faith disclosures about vulnerabilities and preparedness do not expose the firm to liability . . . ." NSHS, *supra* note 10, at 33.

161. Homeland Security Act of 2002, H.R. 5005, 107th Cong. §§ 214(a)(1)(C), (f) (2002).

162. *See, e.g.*, Statement of Copeland, *supra* note 130 (pinpointing uncertainty and

law.[163] Courts hold that FOIA should be "broadly construed in favor of disclosure," and that the nine statutory exemptions should be narrowly construed.[164] Moreover, FOIA is "generally one-sided [in] nature": while a requester who is denied access to government information may file a complaint in a U.S. District Court to enjoin agency disclosure,[165] FOIA typically does not allow private entities to enjoin an agency *from* disclosure.[166] Although these factors cause industry to fear FOIA disclosure of sensitive business information,[167] a clarification of the law,[168] rather than a new blanket exemption that broadens the scope of FOIA's preexisting statutory exemptions, should quiet industry's concerns.

1. The CIIA FOIA exemption expands the breadth of preexisting statutory exemptions that already protect infrastructure data

FOIA's preexisting exemption framework protects adequately the integrity of sensitive data.[169] Specifically, four of the statutory exemptions already in place could protect against the release of critical infrastructure information:[170] 1. Classified Information;[171]

high levels of risk as reasons why industry is reluctant to voluntarily share critical infrastructure information with the government, and arguing that "corporations should not be required to accept such risks . . . in an attempt to protect the public interest").

163. Stohs, *supra* note 132, ¶ 10 (citing Dep't of Interior v. Klamath Water Users Protective Ass'n, 532 U.S. 1, 7 (2001)); *see also* Nat'l Wildlife Fed'n v. U.S. Forest Serv., 861 F.2d 1114 (9th Cir. 1988) (holding that disclosure under FOIA is the rule and secrecy is the exception).

164. *See* Stohs, *supra* note 132, ¶ 10 (citing Anderson v. Dep't of Health & Human Servs., 907 F.2d 936, 941 (10th Cir. 1990), and Sharyland Water Supply Corp. v. Block, 755 F.2d 397, 398 (5th Cir. 1985)).

165. Stohs, *supra* note 132, ¶ 11 (citing 5 U.S.C. § 552(b)).

166. *Id.* (emphasis added) (citing Chrysler Corp. v. Brown, 441 U.S. 281, 316 (1979)). However, an exception may apply to information falling under Exemption 4. *See* discussion *infra* Part IV.B.1 (discussing "reverse-FOIA" suits).

167. *See* Statement of Kallstrom, *supra* note 10 (arguing that the private sector refuses to share sensitive information with the government because of "well-founded fears" that it will ultimately be disclosed under FOIA). *But see* Stohs, *supra* note 132, ¶ 14 (arguing that private sector fears are overstated and that industry's concerns should not bar disclosure of critical infrastructure information).

168. *See* Statement of Tritak, *supra* note 155 (arguing that industry must be presented with "clear, well-defined rules," and that the absence of such a clarification could place our nation at risk).

169. *See generally* Gidiere & Forrester, *supra* note 2 (providing evidence that exemptions 1 through 4 could protect adequately sensitive critical infrastructure data). The Gidiere & Forrester article was one of the first post-September 11, 2001 efforts to assess the possibility of safeguarding sensitive national security information under FOIA's preexisting exemption framework.

170. *See id.* at 139 (arguing that there are ways to work within the confines of the current exemptions to address recent security concerns).

171. *Id.* at 141. "Exemption 1 protects information classified pursuant to an applicable executive order." *Id.*

2. Internal Agency Procedures;[172] 3. Information Exempted by Statute;[173] and 4. Confidential Business Information.[174] Of these four exemptions, Exemptions 1 and 4 would appear to be the most effective preexisting exemptions to secure the integrity of critical infrastructure data. Used in conjunction, these exemptions should provide the courts with tools to protect sensitive infrastructure information, thus eliminating the need for the broad new DHS exemption.

Exemption 1, the "oldest and most well-established ground for withholding government information,"[175] provides for the protection of documents that are "specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy and are in fact properly classified pursuant to such Executive Order."[176] Courts rely heavily upon an

172. Exemption 2 "applies to information 'related solely to the internal personnel rules and practices of an agency.'" *Id.* at 142 (citing 5 U.S.C. § 552(b)(2) (2002)). In the wake of September 11, 2001, DOJ's Office of Information and Privacy supported agency use of this exemption to protect critical infrastructure information. *See id.* at 143 (arguing that while this exemption could be used to justify withholding homeland security information that originated within the agencies, it may not protect records submitted "by a private entity regarding nonagency assets").

173. "Exemption 3 protects information 'specifically exempted from disclosure by statute . . . provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld.'" *See id.* at 145 (citing 5 U.S.C. § 552(b)(3) and reporting that the Critical Infrastructure Information Security Act of 2001, S. 1456, was a Senate "attempt to use Exemption 3 to protect certain homeland security information").

174. "Exemption 4 of FOIA exempts from disclosure 'trade secrets and commercial or financial information obtained from a person and privileged or confidential.'" *See* Gidiere & Forrester, *supra* note 2, at 143 (citing 5 U.S.C. § 552(b)(4) and arguing that Exemption 4 appears to protect critical infrastructure information submitted by private industry regarding vulnerabilities). Gidiere and Forrester base their analysis on cases that find that information voluntarily submitted to the government would receive Exemption 4 protection if it is the type of information that "would customarily not be released to the public by the person from whom it was obtained." *Id.* (citing Critical Mass Energy Project v. NRC, 975 F.2d 871, 878 (D.C. Cir. 1992)). Gidiere and Forrester reason that information that is voluntarily submitted "is not the type of information that would be 'customarily released' by the business." *Id.* at 143. Importantly, this standard for voluntarily submitted business information has not been adopted by all federal circuits. *Id.* It appears that by enforcing this standard, courts would eliminate the need for the broad DHS exemption to protect private industry. *See id.* at 145 (arguing that perhaps the federal circuits should adopt the *Critical Mass* test for voluntarily submitted business information in order to clarify the law protecting "certain homeland security information").

175. *See* Faust, *supra* note 21, at 617 (citing 1 J. O'REILLY, FEDERAL INFORMATION DISCLOSURE 4-11, 11-1 (1983)). Incidentally, FOIA supporters often criticize the use of Exemption 1 to restrict public access to such a magnitude of data. *See id.* at 617 (citing O'Reilly, *supra* note 175, at 11-2).

176. *A Blackletter Statement of Federal Administrative Law*, *supra* note 33, at 64.

agency's affidavit concerning its Exemption 1 classifications.[177] As a result, FOIA litigation rarely results in judicial compulsion to disclose classified records.[178] Therefore, the use of Exemption 1 should protect from disclosure classified records pertaining to critical infrastructure.[179]

Cases suggest that Exemption 4, which applies to "'trade secrets' and to 'commercial or financial information obtained from a person and privileged or confidential,'"[180] already protects critical infrastructure information.[181] In *Critical Mass Energy Project v. Nuclear Regulatory Commission*,[182] the D.C. Circuit held that the purpose of Exemption 4 is to encourage cooperation between the government and companies with useful information.[183] This purpose is the same goal as the FOIA provision in the CIIA.[184] Indeed, agencies safeguard the confidentiality of critical infrastructure information using Exemption 4,[185] including power plant safety reports[186] and design drawings of airplane parts.[187] Exemption 4 even contains a unique provision to protect companies against agency release of information: private companies submitting sensitive information to the government can bring a "reverse-FOIA" suit seeking to enjoin disclosure under the Administrative Procedure Act.[188] This power could provide industry the sense of security it needs to share its proprietary records.

---

177. *Id.* *See generally* Faust, *supra* note 21 (emphasizing the need for effective judicial review of Exemption 1 withholdings in case agencies make improper disclosure decisions).

178. *See* Faust, *supra* note 21, at 629 (citing 128 CONG. REC. S4211 (daily ed. Apr. 28, 1982) (remarks of Sen. Durenberger)).

179. *See* Gidiere & Forrester, *supra* note 2, at 141 (arguing that the current Executive Order protecting critical infrastructure (Executive Order 12958) would likely cover homeland security information, especially when considered in conjunction with other exemptions); *see also* Kimberly, *supra* note 69 (providing for classification of sensitive government information under Executive Order 12958); *supra* note 96 (implementing Executive Order 12958 for DHS).

180. *A Blackletter Statement of Federal Administrative Law*, *supra* note 33, at 65.

181. Summerill, *supra* note 37, at 28.

182. 975 F.2d 871 (D.C. Cir. 1992).

183. *Id.* at 878.

184. Stohs, *supra* note 132, ¶ 13; *see* Gidiere & Forrester, *supra* note 2, at 143 (describing Exemption 4 as protecting "infrastructure information" voluntarily submitted to the government by private industry).

185. Statement of Leahy, *supra* note 89 (referring to the exemption for financial or commercial information (Exemption 4) and citing Critical Mass Energy Project v. Nuclear Regulatory Comm'n, 975 F.2d 871 (D.C. Cir. 1992)).

186. *See id.* (citing *Critical Mass*, 975 F.2d at 874).

187. *See id.* (citing United Tech. Corp. v. F.A.A., 102 F.3d 688 (2d Cir. 1996)).

188. *See* Stohs, *supra* note 132, ¶ 12 n.36 (citing the Administrative Procedure Act, 5 U.S.C. § 706(2)(A) (2002) which suggests that "agency actions will only be overturned if found to be arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with the law").

Aside from mere redundancy, the CIIA FOIA exemption actually goes beyond the scope of the nine statutory exemptions in restricting access to government data. The CIIA's FOIA language is so broad that it could be construed to protect information that would not otherwise be exempt from disclosure.[189] In a minority opinion, four of the nine members of the House Select Committee on Homeland Security expressed concerns that the broad definitions of critical infrastructure and voluntary submission could cover corporations seeking liability protection, such as an energy company hiding information about a leak at its nuclear power plant, simply by voluntarily submitting infrastructure information to DHS.[190] Administrative law expert Jeffrey S. Lubbers provides one possible solution to restrict this overly broad provision: amend the Act to apply to "[i]nformation provided voluntarily by non-Federal entities or individuals . . . *to the extent that it relates to* infrastructure vulnerabilities."[191] This would at least follow FOIA legal precedent by providing for the segregability[192] of information not directly relating to critical infrastructure vulnerabilities.[193]

There are other indications that the CIIA FOIA provision actually expands the preexisting exemption framework. First, the new DHS

189. *See* Robert Leger, *New Congress Threatens Public Records: A GOP-Controlled Legislature May Be Bad News for Open Government*, THE QUILL, Dec. 2002, at 5 (arguing that due to the Act's broad definitions of critical infrastructure and voluntary submission, DHS will "exempt many more documents than are withheld" currently under Exemption 4).

190. H.R. REP. NO. 107-609, at 220 (2002). The House Select Committee on Homeland Security minority view advocated for complete removal of the CIIA FOIA provision, arguing that any new exemption is unnecessary and represents a retreat from openness in government. *Id.* Critics worry that critical infrastructure owners and operators "will be able to submit any information to the government regarding previous attacks in order to become insulated against civil liability related to those attacks." *See* Stohs, *supra* note 132, ¶ 18 (asserting that while the DHS FOIA language will encourage public-private partnerships, it will also inhibit the public's ability to use legal action to enforce industry accountability). In turn, this could decrease private preparedness for future terrorist attacks—if industry knows it will be exempt from civil liability "by simply submitting information regarding the attack" to DHS, it may have "less of an economic incentive to invest in preventing future attacks." *Id.* ¶ 19.

191. *Administrative Law, Adjudicatory Issues, and Privacy Ramifications of Creating a Department of Homeland Security: Hearing Before the Subcomm. on Commercial & Admin. Law of the House Comm. on the Judiciary*, 107th Cong. (2002) (statement of Jeffrey S. Lubbers, Fellow in Law and Government, Washington College of Law) (emphasis added) [hereinafter Statement of Lubbers]. This language is very similar to the Leahy Compromise text. *See Amendment*, *supra* note 109 (limiting the DHS FOIA exemption to records pertaining to "the vulnerability of and threats to critical infrastructure").

192. *See* Envtl. Prot. Agency v. Mink, 410 U.S. 73 (1973) (holding that agencies may disclose nonsecret factual portions of protected records).

193. *See* Statement of Lubbers, *supra* note 191.

exemption supersedes state access laws.[194] Congressman Mark Udall, who voted in favor of the HSA, cited this provision as part of his argument that the CIIA FOIA provision is "unnecessary."[195] Moreover, the Administration's encouragement of nondisclosure in light of national security concerns could directly contradict Congressional intent: Congress explicitly instructed in FOIA that for national security purposes, "only information *specifically exempted from disclosure as national security information by executive determination* may be withheld from the public."[196] Also troubling is the CIIA FOIA provision allowing for the criminal prosecution of federal employees who disclose this voluntarily submitted information.[197] Finally, the CIIA's provision for rendering voluntarily submitted information "off limits for any government regulatory action or civil lawsuit" expands the breadth of the FOIA exemptions further than ever before.[198] This immunity provision could prove to be harmful to the public interest and even endanger public safety.

2. The CIIA FOIA exemption could harm public safety

Although critical infrastructure owners and operators argue that they need this exemption to encourage them to share sensitive information,[199] industry's concerns must be weighed against the operating principles of FOIA and the public's right to access this information. Not only could the exemption undermine government transparency[200] by allowing the government to shield information

194. *See* Homeland Security Act of 2002, H.R. 5005, 107th Cong. § 214(a)(1)(E) (2002).

195. *See* 148 CONG. REC. E1506-02 (daily ed. Sept. 5, 2002) (statement of Rep. Udall) (arguing that the preemption of state access laws is an unnecessary harm caused by the CIIA FOIA exemption when the preexisting exemption framework "does not require the disclosure of national security information, sensitive law enforcement information, or confidential business information").

196. *See* Schoenhard, *supra* note 1, at 506 (emphasis added) (citing this possibility as an example of how the Bush Administration is unjustly restricting the flow of information to the requesting public and arguing that the current security threat does not require a new legal regime).

197. Homeland Security Act of 2002, H.R. 5005, 107th Cong. § 214(f) (2002); *see* Clift, *supra* note 116 (citing this provision as an example of how the DHS FOIA provision chips away at FOIA and describing the provision as an indication that the Republicans "went further than anybody imagined" in eroding FOIA).

198. *See* Leger, *supra* note 189 (arguing that the provision would expand beyond Exemption 4 and cautioning that the ramification is that industry would be allowed to "dump information about any mistakes, which would forever be hidden from the public").

199. *See* discussion *supra* Part IV.B.

200. *See* Thomas Blanton, *The World's Right to Know*, FOREIGN POL'Y, July 1, 2002, at 50 (arguing that the concept of freedom of information and the attendant result of transparency in government has evolved from "a moral indictment of secrecy to a tool for market regulation . . . efficient government, and economic . . . growth"). *But*

from public view, but this legislation could also needlessly risk public safety.[201] In Congressional debate, Senator Leahy posed the following scenario: if DHS receives information from a biomedical laboratory about a security vulnerability and anthrax is released subsequently from the laboratory as a result of that vulnerability, DHS would not be able to disclose under FOIA information relating to this security vulnerability without first securing the laboratory's consent to release the information.[202] Moreover, due to the civil immunity guaranteed by the CIIA,[203] if a company submits information that its factory is leaking arsenic into ground water, that information cannot be turned over to local health authorities to use in any enforcement proceeding, nor could the public access it through FOIA for use in a civil tort action.[204]

As enacted, the law could "'tie the government's hands' by precluding it from taking civil enforcement action against a company by 'direct use' of information obtained through critical infrastructure" reports.[205] Therefore, Senator Leahy argued, the civil immunity provided under the CIIA provides industry with a "perfect blueprint" to avoid liability by allowing companies to feed damaging information into the voluntary disclosure system, thus eliminating the possibility for the government or others harmed by the company's actions to use that information against the company.[206] This result, permissible under the CIIA, could endanger public safety rather than

---

see Moon, *supra* note 25, at 1167-68 (arguing that the principle of transparency in government is a liberal construction).

201. *See, e.g.*, Statement of Leahy, *supra* note 89, at S11426 (emphasizing that the DHS FOIA provision provides a broad FOIA exemption "without making any real gains" in national security); Stohs, *supra* note 132, ¶ 4 (arguing that the CIIA FOIA exemption could threaten public access to vital public health and safety information); Krebs, *supra* note 103 (quoting James X. Dempsey, deputy director for the Center for Democracy and Technology, as arguing that private industry could "shield vital health and safety information from the public, even if disclosure of the information would pose no threat whatsoever").

202. Statement of Leahy, *supra* note 89, at S11425.

203. Homeland Security Act of 2002, H.R. 5005, 107th Cong. § 214(a)(1)(C) (2002).

204. Statement of Leahy, *supra* note 89, at S11425. For an elaborate set of hypothetical scenarios illustrating potential consequences of the CIIA FOIA exemption, see Steinzor, *supra* note 93, at 656-58 (discussing the potential implications of the CIIA on transportation security, pollution, corporate fraud, and various other threat scenarios).

205. *See* Dan Caterinicchia, *Sharing Seen as Critical for Security*, FED. COMPUTER WK. (May 9, 2002) (quoting John Malcolm, Deputy Assistant Attorney General), *at* http://www.fcw.com/fcw/articles/2002/0506/web-crit-05-09-02.asp (on file with the American University Law Review).

206. Statement of Leahy, *supra* note 89, at S11425; *see* Caterinicchia, *supra* note 205 (quoting John Malcolm, Deputy Assistant Attorney General, as stating that a "company that was knowingly at fault" could "do a 'document dump' on the government and basically absolve itself of future civil prosecution").

preserve it. Such a tactic would not require that company to address the reported vulnerability. The ensuing lack of public accountability could eliminate industry's incentives to correct security problems. [207] Moreover, this tactic could also deprive the public of information on how to protect itself from reported hazards. [208]

The goal of the new exemption is clear: to encourage private industry to share sensitive information with the government in order to assist the government in preventing and responding to terrorist threats. Yet the CIIA FOIA provision goes far beyond this goal, containing language so broad that it creates the potential for abuse. This is an unacceptable result when, in all likelihood, this broad exemption will not secure private industry's cooperation in public-private information sharing partnerships.

3. Even with new protections, future prospects of public-private information sharing remain uncertain

a. Distrust and uncertainty continue to present obstacles to voluntary information sharing

Although the Bush Administration aims to foster public-private information sharing,[209] establishing trusting relationships between the public and private sectors remains a difficult task.[210] The protections

207. *See* Steinzor, *supra* note 93, at 664. Steinzor's article provides an extensive analysis of the CIIA's potential implications for corporate accountability and public safety.

208. *See id.*

209. *See* NSHS, *supra* note 10, at 31 (declaring that the U.S. will facilitate an "unprecedented level of cooperation . . . with private industry" in order to reduce the nation's vulnerability to terrorism); *see also* NSPPCIKA, *supra* note 6, at vii (stating that homeland security is a "shared responsibility" for the federal government, state and local governments, and the private sector). Government and industry officials alike agree that public-private information sharing will be necessary to protect the homeland. *See, e.g.*, Statement of Dacey, *supra* note 125 (arguing that information sharing partnerships are necessary for developing approaches to defend against cyber attacks); Statement of Miller, *supra* note 156 (stating that the Information Technology Association of America, which represents information technology and communications companies, supports the government's goal of increasing public-private information sharing); Statement of Tritak, *supra* note 155, at 77 (arguing that "infrastructure assurance can only be achieved by a voluntary public-private partnership"); Caterinicchia, *supra* note 205 (reporting Senator Robert Bennett's statement that because the private sector and government are both targets, "they should be talking to each other," but that industry fears disclosed information could be used against them).

210. *See Critical Infrastructure Protection: Who's In Charge?: Hearing of the S. Governmental Affairs Comm.*, 107th Cong. 23-24 (2001) (statement of Jamie S. Gorelick, Vice Chairperson, Fannie Mae) (asserting that there is "a decided lack of trust between industry and government"). Supporting this assertion, the Brookings Institution argues that the intersection between the Federal government and the private sector poses some of the country's "most difficult homeland security

offered by the CIIA are unlikely to eliminate the many obstacles to voluntary information sharing.[211] *Trust* is critical to successful partnerships,[212] and industry officials argue that it can only be built over time.[213] Thus, the government faces the challenge of initially establishing and maintaining trust relationships as it scrambles to shore up national security.[214] As it stands, private industry is reluctant to confirm security breaches due to "competitive pressure, fear of regulations, and simple embarrassment."[215] This makes cooperation a difficult endeavor, especially because such partnerships typically form only in times of imminent crisis.[216]

---

challenges." *See* THE BROOKINGS INSTITUTION, *supra* note 151, at 8 (calling for new public-private partnerships without imposing "undue economic costs" on private industry); *see also* GENERAL ACCOUNTING OFFICE, CRITICAL INFRASTRUCTURE PROTECTION: COMPREHENSIVE STRATEGY CAN DRAW ON YEAR 2000 EXPERIENCES 24 (Oct. 1999) [hereinafter GAO Y2K] (reporting that the task of establishing public-private partnerships poses a significant challenge for critical infrastructure protection).

211. *See* Caterinicchia, *supra* note 205 (quoting John Tritak, director of the Critical Infrastructure Assurance Office, as stating that "[p]eople expect too much of legislation to fix a cultural problem"). Impediments to information sharing include a lack of trust between private industry and government and industry's reluctance to share sensitive information due to concerns that public release of that information could undermine customer confidence, open the floodgates to litigation, and harm business in general. *See* GAO IS, *supra* note 154, at 7; *see also* discussion *supra* Part IV.B (describing industry's reluctance to share sensitive information with the government and citing industry's call for increased protections).

212. GAO IS, *supra* note 154, at 7. Along that vein, Tritak argues that while a narrowly crafted FOIA exemption might facilitate information sharing, the critical factor is still trust. *See* Statement of Tritak, *supra* note 155, at 77 (arguing that achieving trust is "no small challenge").

213. GAO IS, *supra* note 154, at 2.

214. *See id.* at 14-15 (arguing that the government should take steps to institutionalize trust, rather than depend on personal relationships with separate industries); *see also* Statement of Tritak, *supra* note 155, at 78 (stating that trust in any voluntary information sharing relationship "requires a predictable and stable process where the outcomes are certain").

215. *See* Kerber, *supra* note 117 (discussing disincentives to information sharing, while arguing for joint law enforcement and business cooperation in order to protect critical infrastructure from would-be hackers and terrorists).

216. *See id.* (quoting John Woodward, Director of Information Warfare at Mitre Corp.); *see also* Statement of Miller, *supra* note 156, at 95 (reporting that although ninety percent of large corporations and government agencies responding to a 2002 FBI/Computer Security Institute Survey detected computer security breaches between May 2001 and May 2002, only forty-four percent were "willing and/or able to quantify their financial losses"); *House Voting on Homeland Security with FOIA, Privacy Provisions*, WASH. INTERNET DAILY, July 19, 2002 (quoting Entrust C.E.O. William Conner as stating that of the aforementioned ninety percent of private sector companies, only thirty-four percent reported cyber attacks to law enforcement); Krebs, *supra* note 103 (explaining that Alan Paller, director of research for the SANS Institute, believes that most companies will continue to be reluctant to share information on system vulnerabilities with the government, even with the newly-enacted FOIA exemption, because industry traditionally does not share such sensitive critical information unless the recipient party could help solve the problem).

Even with the CIIA FOIA exemption in place, industry must still focus its efforts on staying in business.[217] To meet the public interest goal of public-private cooperation,[218] companies would have to use their valuable resources to develop proprietary information regarding vulnerabilities.[219] This appears to be contrary to the operational goals of profit-driven organizations, because it will not increase short-term profits.[220]

Information sharing between the public and private sectors is both laudable and necessary,[221] and many believe that a successful strategy for homeland security depends on "the ability of all levels of government and the private sector to communicate effectively with one another."[222] Yet as it stands, the government could find its efforts in the CIIA wasted without securing industry's infrastructure disclosures.[223] Ineffective collaboration undermines efforts to protect

---

217. *See* discussion *supra* Part IV.B (discussing demands on industry to keep its companies in business during tough economic times).

218. *See* Caterinicchia, *supra* note 205 (quoting John Tritak, director of the Critical Infrastructure Assurance Office, as stating that "[b]oth government and industry realize that sharing information is 'in the public interest'").

219. Stohs, *supra* note 132, ¶ 20.

220. *Id.* (noting that "such investments may be hard to come by with the current economic slowdown"); *see, e.g.*, Frye, *supra* note 123, at 364 (arguing that because "profit motivates all private sector activity; privately operated systems respond to market motivators rather than public good"). For example, if a financial institution faces a cyber attack, its profit-driven response should simply be to quickly stop the attack: it would not be "cost-effective for businesses to invest in anything other than stopping 'the problem' and just getting on with business." *See id.* at 366 (quoting DAVID KEYES, JOINT ECON. COMM. OF THE U.S. CONG., SECURITY IN THE INFORMATION AGE: NEW CHALLENGES, NEW STRATEGIES, 46 (2002), *available at* http://www.house.gov/jec/security.pdf (on file with the American University Law Review). Frye cites the notorious 1995 Citibank hacking, in which hackers stole $10 million, as the only case in which a bank has acknowledged a computer hacking resulting in financial loss. Frye, *supra* note 123, n. 99. Frye concludes that the private sector should not be criticized for responding to such "naturally occurring incentives" in a free-market economy; rather, the public and private sectors should work together to tailor the private sector's motivations and duties toward meeting the goal of "reasonable preparedness and full disclosure." *Id.* at 376; *see also* THE BROOKINGS INSTITUTION, *supra* note 151, at 4 (arguing that "the business of business is business, not homeland security" and citing the chemical and trucking industries as examples of sectors that have not taken adequate steps on their own to improve security).

221. *See* NSHS, *supra* note 10, at 55 (describing information as "a vital foundation for the homeland security effort"). The White House's *National Strategy for Homeland Security* includes as its "National Vision" the goal of building a "national environment that enables the sharing of essential homeland security information" that would give homeland security officials "complete and common awareness of threats and vulnerabilities." *Id.* at 56.

222. GAO DHS, *supra* note 86, at 17; *see also* NSPPCIKA, *supra* note 6, at 12 (asserting that information sharing between the government and private industry is necessary to mitigate terrorist threats).

223. *See* Stohs, *supra* note 132, ¶¶ 4, 20 (arguing that this provision may not "do anything to increase public/private collaboration" and that the "biggest roadblock to public/private information sharing still remains: overcoming business interests"); *see* discussion *supra* Part IV.C.3 (discussing cultural impediments to information sharing,

our nation's critical infrastructure from terrorist attacks.[224] One alternative to voluntary disclosures is to *require* information sharing between the public and private sectors.[225] Such information likely would still receive protections under Exemption 4: information that is required to be submitted to the government receives Exemption 4 protection "if it is of the sort not customarily released," and if that disclosure would either "impair the government's ability to obtain necessary information in the future," or "cause substantial harm" to the submitting party.[226] It appears that sensitive critical infrastructure data would meet this criterion and thus be afforded Exemption 4 protection. In light of our infrastructure vulnerabilities, perhaps lawmakers should consider this option.[227] Prior public-private partnerships provide further options for dealing with the information sharing problem.

b. Lessons From Prior Successful Partnerships Could Provide the Government With a Blueprint to Facilitate Information Sharing

The notion of public-private partnerships is not an entirely new idea: the Clinton Administration provided a blueprint for public-private information sharing on critical infrastructure matters through issuance of Presidential Decision Directive 63 ("PDD 63"), entitled "Protecting America's Critical Infrastructures."[228] In light of our country's increased dependence on interconnected infrastructures, PDD 63 advocated for the voluntary participation of private industry in public-private partnerships as one means of securing sensitive sectors.[229] In so doing, PDD 63 encouraged private industry to establish Information Sharing and Analysis Centers to serve as a means of gathering, analyzing, and disseminating information

such as trust, that cannot be legislated by statute).

224. GAO DHS, *supra* note 86, at 17.

225. Stohs, *supra* note 132, ¶ 21.

226. *See id.* ¶ 21 & n.48 (citing Pub. Citizen Health Research Group v. Food & Drug Admin., 185 F.3d 898, 903 (D.C. Cir. 1999)); *A Blackletter Statement of Administrative Law*, *supra* note 33, at 65-66.

227. *See* Stohs, *supra* note 132, ¶ 21 (arguing that because Exemption 4 could still cover information submitted voluntarily to the government, this option deserves discussion).

228. The White House, Office of the Press Secretary, *Fact Sheet: Protecting America's Critical Infrastructures: PDD 63* [hereinafter PDD 63], *at* http://www.fas.org/irp/offdocs/pdd-63.htm (May 22, 1998) (on file with the American University Law Review). The White House issued this explanation of PDD 63 because the original document is classified.

229. *Id.*; *see* GAO Y2K, *supra* note 210, at 5 (declaring that PDD 63 acknowledged that public-private cooperation would be necessary in order to evaluate cyber-risks to our critical infrastructure).

between private infrastructure sectors and the government.[230] Following this blueprint, the Bush Administration's *National Strategy for Homeland Security*, released on July 16, 2002, assigned certain agencies the "primary responsibility for interacting with critical infrastructure sectors" in order to facilitate information sharing.[231] For example, under the Bush Administration's plan, DHS will interact with the Information, Telecommunications, and Emergency Services sectors, whereas the Department of Health and Human Services will interact with the Public Health sector.[232]

One example of successful public-private information sharing is the National Security Telecommunications Advisory Committee ("NSTAC"), created in 1982 by Executive Order 12382 ("President's National Security Telecommunications Advisory Committee").[233] NSTAC's industry members provide advice to the federal government on national security and emergency preparedness telecommunications matters.[234] For over twenty years, this advisory board has voluntarily advised the country's leaders on security issues regarding the telecommunications and information infrastructure.[235] As such, NSTAC stands as a model for public-private collaboration.[236] As an advisory board, however, NSTAC is not responsible for sharing with the government individual members' infrastructure vulnerabilities.

Perhaps the best known and most successful endeavors of information sharing on system vulnerabilities were the public-private partnerships formed between the government and private computer network operators in response to the potential Year 2000 ("Y2K") date conversion problem.[237] One possible reason why industry complied voluntarily with the government's information requests was that Congress enacted a narrowly tailored FOIA provision that

230. PDD 63, *supra* note 228; GAO IS, *supra* note 154, at 6. In 2001, GAO reported that progress in implementing PDD 63 has been slow. *See id.* (citing the creation of six Information Sharing and Analysis Centers in five industry sectors).

231. NSHS, *supra* note 10, at 31.

232. *Id.* at 32.

233. NSTAC RESPONSE, *supra* note 152, at *14.

234. *Id.*

235. *Id.*

236. Similar to NSTAC, the Treasury Department chairs the Financial and Banking Information Infrastructure Committee, which bridges a public-private partnership focusing on security issues concerning the financial services industry. NSHS, *supra* note 10, at 31.

237. *See* GAO Y2K, *supra* note 210, at 3 (summarizing the Y2K challenge as "a major test of our nation's ability to protect its computer-supported critical infrastructures"). *See generally* NSTAC TASK FORCE REPORT, *supra* note 157, at 7-8 (describing the Y2K disclosure system and arguing that it was a successful example of public-private information sharing).

exempted such information from public disclosure.[238] Also, Y2K information sharing was successful in part because private industry and the government together "recognized the threat and faced a fixed deadline by which time[ly] action had to be taken."[239] This is different from sector-wide critical infrastructure protection, where industry faces an unclear threat for a potentially infinite duration.[240]

One key lesson from the Y2K success story is that industry's long-standing disclosure concerns[241] make it reluctant to form information sharing partnerships without certain protections. Thus, in order to encourage information sharing, the government should take some action to demonstrate the importance it places on protecting industry's sensitive business information.[242] Industry was unconvinced that FOIA's preexisting statutory framework protected adequately the integrity of critical infrastructure data.[243] An official clarification of FOIA's preexisting exemption framework could address these concerns.[244] However, if the government decides that it needs to provide a greater incentive in order to strengthen national security, the narrow FOIA exemption proposed by the Senate compromise legislation provides a palatable alternative.[245] Regardless, the

238. Public Law 105-271, the "Year 2000 Information and Readiness Disclosure Act," provides that "any Year 2000 statements or other such information provided by a party in response to a special Year 2000 data gathering request . . . shall be exempt from disclosure under . . . the 'Freedom of Information Act.'" Year 2000 Information and Readiness Disclosure Act, Pub. L. No. 105-271, § 4(f)(3)(A), 112 Stat. 2386 (1998). NSTAC recommends legislation similar to this Act that would protect critical infrastructure information voluntarily shared from disclosure under FOIA, arguing that none of the preexisting exemptions would cover critical infrastructure information. NSTAC TASK FORCE REPORT, *supra* note 157, at 9, 11.

239. *Id.* at 8.

240. "Without a clear and present danger, it is difficult for industry to justify spending additional dollars" to protect its systems. *Id.* Unlike the Y2K problem and its finite end-date, the challenge of securing our nation's critical infrastructure protection continues. GAO Y2K, *supra* note 210, at 20. Similar to Y2K, ongoing critical infrastructure protection will require both public and private sector involvement. *Id.* at 18.

241. *See* discussion *supra* Part IV.B (citing industry's liability concerns as preventing it from forming public-private partnerships).

242. Statement of Tritak, *supra* note 155. This assertion is supported by Harris Miller, President of the Information Technology Association of America, who testified in a Senate Governmental Affairs Committee hearing that uncertainty has a "chilling effect" on information sharing and that government must give private industry certainty that its sensitive information would be protected. Statement of Miller, *supra* note 156, at 98.

243. Miller testified that the preexisting FOIA language was not sufficient to protect critical infrastructure data from disclosure and advocated for "the extraordinary treatment of a complete ban on FOIA disclosure." *Id.* at 102.

244. *See supra* note 167 and supporting text (discussing the necessity of a clarification of current FOIA law).

245. *See* discussion *supra* Part III.B (reviewing the compromise legislation's narrower FOIA language and absence of immunity provisions).

government should pay attention to demands for reform[246] and act to restrict the CIIA's overly broad FOIA language.[247]

4. The recent erosion of FOIA is a sleeper issue that could shock the public

Following the terrorist attacks on September 11, 2001, the public entrusted the government to protect national security and might be reluctant to question, or may not even be aware of, the attendant reduction of civil liberties.[248] The ramifications of the Bush Administration's FOIA guidance, geared toward agencies, were not widely reported in the mainstream news media.[249] Similarly, the controversy surrounding DHS labor rules often eclipsed the CIIA FOIA debate on Capitol Hill.[250]

The Bush Administration must not mistake the American public's apparent complacency on this matter as tacit approval of expansion of governmental secrecy. With DHS now serving as the figurehead for the nation's counter-terrorism efforts, expectations of enhanced national security fall squarely upon its shoulders. The public is already skeptical about DHS's ability to safeguard our nation.[251] One terrorist attack would intensify public scrutiny and raise questions as

246. *See Fix This Loophole*, WASH. POST, Feb. 10, 2003, at A20 (imploring Congress to quickly eliminate the overly broad language of the DHS FOIA provision before the government and the public find themselves "out of the loop—on important regulatory matters").

247. *See* discussion *supra* Part IV.C.1 (reviewing the DHS FOIA provision's overly broad language and arguing that it must be more narrowly tailored so as not to create the potential for abuse).

248. *See* Statement of Swire, *supra* note 89, at 23 (expressing concern that if everyone is concerned with short-term gains to homeland security, it is a question whether people will voice "long-time concerns about erosions of civil liberties").

249. *See* Travis Loop, *State of the Union's Press*, PRESSTIME, Feb. 2003, at 7 (quoting Paul McMasters, First Amendment Ombudsman at the Freedom Forum, as stating that editors must be more vigilant in sharing with readers how government access laws contribute to the stories they read; otherwise, the public will not fully realize how access laws like FOIA affect their daily lives).

250. *See* Leger, *supra* note 189 (defending the media's focus on labor rules as understandable, because disagreement over that provision led to a Senate stalemate). Leger argues that the CIIA FOIA provision "slaps all 281 million Americans" and serves as "Exhibit One" that this Administration will "toss favors to business and industry." *Id.*

251. A Gallup poll from early January 2003 indicated that only thirteen percent of Americans feel "a lot" safer with the new DHS; four in ten Americans feel DHS will not make the country safer at all. *The State of Our Union: Speech Shows Growing Gap Between Bush Rhetoric and Reality*, U.S. NEWSWIRE, Jan. 29, 2003; *see* THE BROOKINGS INSTITUTION, *supra* note 151, at 1 (arguing that the new DHS "will not in and of itself make Americans safer" and pinpointing problem areas within the Bush Administration's homeland security policies). In its assessment of security concerns post-September 11, 2001, the Brookings Institution highlights concerns facing the new DHS, reporting that homeland security proves overwhelming in both its complexity and in the number of potential targets. *Id.* at 2.

to why DHS's mission failed.[252] Chances are DHS *will* somehow fail, because there is no other agency that faces a more difficult task involving such high risks.[253] The public could be outraged to discover that one practical ramification of CIIA FOIA exemption is that the public cannot directly hold DHS—its own government—accountable for its operations.[254]

Popular distrust of government, fueled by scandal, led to FOIA's enactment and fortification.[255] If FOIA's erosion continues unimpeded, an attack on our homeland could ultimately lead to demands for reform.[256] The public is becoming increasingly aware of these new FOIA developments through personal experience in the request process, and through new lawsuits.

D. Current Effects of Post-September 11, 2001 FOIA Restrictions on the Requesting Community

The immediate effects of the post-September 11, 2001 FOIA restrictions on the requesting community are in dispute.[257] Agency officials characterize the effects on FOIA implementation as relatively minor, except for mail delays associated with anthrax in October

252. *See Talkback Live* (CNN television broadcast, Jan. 24, 2003) (quoting DHS Secretary Tom Ridge as stating that DHS has the "unified mission of protecting America").

253. *See* GAO DHS, *supra* note 86, at 5 (arguing that "DHS's national security mission is of such importance that the failure to address its management challenges and programs risks could have serious consequences on our intergovernmental system, our citizens' health and safety, and our economy"). If DHS were to fail at protecting the homeland, this could result in grave consequences for our nation. *Id.* at 3. This challenge is exacerbated by the fact that most of the agencies merged into DHS were created for reasons largely unrelated to the nation's current national security concerns. THE BROOKINGS INSTITUTION, *supra* note 151, at 15. As such, DHS faces the challenge of managing these disparate groups while focusing on the ultimate task of protecting national security. *See id.* at 15-16.

254. If the past is any predictor, FOIA requests often follow disastrous events and even lead to reform. *See, e.g.*, *supra* notes 20 and 27 and accompanying text (citing the Vietnam War and Watergate as events leading to public outrage and cries for reform). Drawing upon this experience, the public would probably file FOIA requests with DHS if any future national security catastrophe occurs.

255. *See id.* (discussing FOIA's enactment during the Vietnam War and FOIA's strengthening after the Watergate scandal).

256. Moreover, such events could damage public officials who support these FOIA policies. Robert Saloschin writes that his FOIA experience taught him that "clinging to secrecy in the face of persistent attack, even if legally warranted, can be very damaging" to government officials—especially if others believe the secrecy to be unwarranted. Saloschin, *supra* note 3, at 1407. Saloschin recalls the Watergate scandal, when President Nixon's withholding of information ultimately led to his resignation. *Id.*

257. *See* GAO, *supra* note 22, at 3 (reporting that agency officials and FOIA requesters view the impact of September 11, 2001, on access to government information differently).

2001.[258] A recent GAO Report surveyed FOIA officers at various agencies and found that most of those officers "did not notice changes in their agencies' responses to FOIA requests compared to previous years."[259] This survey began in October 2002, one year after the policy change initiated by the Ashcroft Memorandum and before Congress created the new DHS. As a result, the survey did not take into account any data regarding the level of disclosures at DHS, the agency most likely to safeguard critical infrastructure information due to the authority it received from the CIIA FOIA provision.

In contrast, members of the requesting community express general concerns about the dissemination of information and access to government information in light of the removal of information from some government web sites after September 11, 2001.[260] Importantly, some requesters characterize DOJ's new policy as "representing a shift from a 'right to know' to a 'need to know'[261] that could discourage the public from making requests."[262] Many Americans are also affected by state decisions that follow the Bush Administration's lead in narrowing the scope of FOIA disclosures.[263]

The long-term effects of the post-September 11, 2001 FOIA restrictions will not be known for some time.[264] "[A]ny effects may not be clear until denials of information during this time period are appealed, litigated, and decided—a process that could take several years."[265] Ultimately, it is simply too soon to determine conclusively whether information requests now receive more scrutiny from all agencies.[266] However, one need only look to the federal courts to find judicial responses to the Bush Administration's new policies.

258. *Id.*
259. General Accounting Office, Freedom of Information Act: Agency Views on Changes Resulting from New Administration Policy 2 (2003) (reporting that one third of the officers surveyed noticed a decreased likelihood of disclosure post-September 11, 2001 and that seventy-five percent of those officers blamed the new Ashcroft policy as the main reason for the change).
260. *Id.*; *see also* Parker, *supra* note 3, at 1A (reporting that the government removed "hundreds of thousands of public documents" from its websites and that it edited other public information); Schoenhard, *supra* note 1, at 502 (criticizing the removal of information from government websites, such as the Department of Energy website, after September 11, 2001).
261. *See* Beierle & Bell, *supra* note 135.
262. GAO, *supra* note 22, at 3; *see also* Beierle & Bell, *supra* note 135.
263. *See* Parker, *supra* note 3 (citing four states' efforts to restrict disclosure laws).
264. GAO, *supra* note 22.
265. *Id.* at 3.
266. Blum, *supra* note 139.

1. Current legal challenges

On the litigation front, current FOIA lawsuits could test the judicial waters of the Bush Administration's new nondisclosure policy.[267] David Vladeck, a Georgetown University Law Center professor and former litigation director of Public Citizen, commented that FOIA results in additional litigation to obtain information that was previously obtainable without a lawsuit.[268] Moreover, the fact that Attorney General Ashcroft has essentially pledged a "more vigorous defense" of agency decisions so long as they are premised on a sound legal basis could pave the way for more difficult courtroom challenges and result in less information being made public.[269]

One FOIA success in the past year resulted from a complaint filed by Judicial Watch regarding a purported anthrax cover-up at the Washington, D.C. Brentwood mail facility.[270] Judicial Watch filed a FOIA request with the U.S. Postal Service ("U.S.P.S.") regarding anthrax information.[271] When the U.S.P.S. failed to comply with the request, Judicial Watch filed suit in the U.S. District Court for the District of Columbia.[272] On September 11, 2002, Judge Henry H. Kennedy, Jr. ordered the U.S.P.S. to "produce all documents or portions thereof which are responsive to Plaintiff's request."[273] Those court-mandated disclosures indicated that U.S.P.S. and U.S. government officials knew that envelopes leaked anthrax into the facility, but those officials failed to close that facility for four more days, after two Brentwood employees died from inhalation anthrax.[274] Based on these FOIA disclosures, Judicial Watch filed a new complaint for a criminal investigation with the U.S. Attorney for D.C.[275]

Recently, in *Electronic Privacy Information Center v. Office of Homeland Security*,[276] the Electronic Privacy Information Center ("EPIC") filed a

267. *See id.* (detailing public interest groups' continuing attempts to secure information under FOIA and reporting the National Resources Defense Counsel general counsel Sharon Buccino's determination to challenge the White House on the issue).

268. *Id.*

269. *See id.* (discussing Ashcroft's FOIA guidance to agencies).

270. Judicial Watch is a public interest group that investigates and prosecutes government corruption and abuse. Anthrax Lawsuit, *supra* note 12.

271. *See Complaint for Criminal Investigation: Anthrax Attacks* (Dec. 6, 2002) (detailing Judicial Watch's FOIA request), *available at* http://www.judicialwatch.org/cases/99/brentwoodltr.htm (on file with the American University Law Review).

272. *Id.*

273. *Id.*

274. *See id.* (listing information revealed in U.S. Postal Service documents).

275. *See* Anthrax Lawsuit, *supra* note 12.

276. No. 02-620 (D.D.C. Dec. 26, 2002), *available at* http://www.epic.org/open_gov/homeland/ohs_decision.pdf (on file with the American University Law

complaint against OHS requesting OHS to process and release records.[277] EPIC made a FOIA request on March 20, 2002, requesting records relating to OHS's proposed programs.[278] OHS responded that it could not be subjected to FOIA requests because it was not an agency.[279] The District Court for the District of Columbia dismissed OHS's motion for summary judgment and granted EPIC's discovery motion.[280]

The Bush Administration will continue to monitor progress in that case, as well as many other unresolved FOIA cases. Pending litigation are cases dealing with the release of names of those detained as part of the investigation into the September 11, 2001, terrorist attacks, statistics on the Justice Department's use of new surveillance powers authorized by the USA PATRIOT Act, information related to the Defense Department's "Total Information Awareness" initiative, and data maintained by U.S. Attorney's offices indicating how many investigations are under way in specific categories, such as terrorism or civil rights.[281] Although the *Judicial Watch* and *EPIC* lawsuits demonstrate judicial compulsion of FOIA disclosure despite the Bush Administration's restricted FOIA policy, the broad new CIIA FOIA exemption indicates that there still remains an overall climate of nondisclosure post-September 11, 2001.

2. Additional legislation in the current congressional term

The CIIA FOIA provision could lead to more debate in the 2003-2004 congressional term. Senator Leahy, a long-time FOIA advocate, argued that the HSA's flaws would need to be addressed in this congressional term.[282] Similarly, Senator Levin declared that he would attempt to legislate FOIA during the 108th Congress to clarify the exemptions under the Act.[283] Indeed, the 108th Congress revisited the FOIA issue through the Senate Governmental Affairs Committee's confirmation hearing of now-DHS Secretary Tom

---

Review).

277. *See id.* (summarizing EPIC's request for documents and subsequent complaint).

278. *See id.* at **1-2 (quoting EPIC's request for information on OHS plans to implement a national system for driver's licenses and to use biometric technology for information purposes).

279. *See id.* at *2 (arguing that the court should dismiss the case for lack of jurisdiction over OHS, a non-agency). FOIA only applies to agency records. *See supra* note 33 and supporting text (defining agency records for FOIA purposes).

280. *Elec. Privacy Info. Center*, No. 02-620, at *1.

281. *See* Blum, *supra* note 139 (detailing public interest groups' use of FOIA to compel a reluctant administration to release information).

282. *See* Statement of Leahy, *supra* note 89, at S11423.

283. *See* Samuelsohn, *supra* note 83.

Ridge.[284] In the hearing, Senator Levin focused on the CIIA's authorization of criminal penalties for those who disclose protected sensitive information.[285] Senator Levin argued for the need to repair the underlying legislation because its criminal penalty and legal immunity provisions could eventually lead companies to protect themselves from legal actions simply by providing infrastructure information to the DHS.[286] Building on that argument, Senator Durbin questioned Secretary Ridge on whether he was aware that the resulting legal immunity would severely limit ordinary citizens' opportunity for legal redress.[287] Secretary Ridge expressed concern about differing interpretations of the statute and stated that he would work with the Senators to clarify the CIIA FOIA language.[288]

Fulfilling the promise to keep the FOIA fight alive in the Senate, Senators Leahy, Levin, Jeffords, Lieberman and Byrd recently proposed new legislation to chisel away the broad barrier to disclosure under the CIIA. Their bill, the Restoration of Freedom of Information Act of 2003,[289] ("Restore FOIA Act") follows closely the Senate compromise legislation that Senators Leahy, Bennett and Levin advanced in Fall 2002. Like the compromise legislation, this measure would limit the CIIA FOIA exemption to "records" submitted by private entities, a much narrower standard than the provision for "information" contained in the CIIA.[290] The bill would

284. *See generally Hearing on the Nomination of Honorable Thomas "Tom" J. Ridge to be Sec'y of the Dep't of Homeland Security Before the S. Comm. On Governmental Affairs*, 108th Cong. (2003).

285. *See Hearing on the Nomination of Honorable Thomas "Tom" J. Ridge to be Sec'y of the Dep't of Homeland Security Before the Senate Comm. On Governmental Affairs*, 108th Cong. 37 (2003) (statement of Sen. Levin, Member, Senate Governmental Affairs Comm.) [hereinafter Statement of Levin] (asserting that the language in the bill regarding unclassified information is too broad because, as written, it might prevent disclosure of information for fear of criminal prosecution); *see also Hearing on the Nomination of Honorable Thomas "Tom" J. Ridge to be Sec'y of the Dep't of Homeland Security Before the Senate Comm. On Governmental Affairs*, 108th Cong. 41 (2003) (statement of Sen. Durbin, Member, Senate Governmental Affairs Comm.) [hereinafter Statement of Durbin].

286. *See* Statement of Levin, *supra* note 285, at 37 (describing this opportunity as a "security blanket" for the companies).

287. *See* Statement of Durbin, *supra* note 285, at 41 (arguing that he understands the need to protect sensitive information, but that the CIIA exceeded that by rendering companies immune from litigation merely by making disclosures to the DHS).

288. *See Hearing on the Nomination of Honorable Thomas "Tom" J. Ridge to be Sec'y of the Dep't of Homeland Security Before the Senate Comm. On Governmental Affairs*, 108th Cong. 37, 41 (2003) (statement of Tom Ridge, Nominated to be Secretary of Homeland Security) (arguing that it was not the intent of those who crafted the CIIA FOIA exemption to protect wrongdoers, and that setting up the DHS' information analysis and infrastructure protection unit would be one of his initial tasks).

289. S. 609, 108th Cong. (2003).

290. Whereas records "refer to physical and well-defined communications," such

restrict the CIIA FOIA exemption to records pertaining to "the vulnerability of and threats to critical infrastructure (such as attacks, response and recovery efforts)," [291] whereas the current CIIA FOIA exemption applies to any "critical infrastructure information." In contrast to the CIIA's broad prohibition against disclosure, including criminal penalties against any government employee who releases that information for any reason, the Restore FOIA Act eschews criminal penalties and would not forbid the use of these records in civil court cases in order to hold companies accountable for their wrongdoing or to protect the public. [292] The bill was referred to the Senate Judiciary Committee in March 2003 and awaits further consideration.

With continuous lawsuits to compel the release of FOIA information by the Bush Administration, as well as efforts to narrow the broad CIIA FOIA language in this congressional term, a clear exposition of the public's rights under FOIA in our country is far from complete.

CONCLUSION

FOIA is a critical component of our democratic government and should be protected even in times of heightened concerns about national security.[293] Implemented in 1966, FOIA survived the national security crises of the Cold War without imposing severe restrictions on the dissemination of government information. Governmental transparency and homeland security are not inconsistent goals. Preexisting statutory exemptions, in particular the first and fourth exemptions, provide broad protection of sensitive information, even after September 11, 2001.[294]

Present and future efforts to erode FOIA will harm requesters who

---

as documents and reports, "information" is a more expansive, undefined term and could encompass telephone calls, conversations, or other non-traditional communications. *See* U.S. Senator Patrick Leahy, *Side-by-Side Analysis of the Leahy-Levin-Jeffords-Lieberman-Byrd Restoration of Freedom of Information Act of 2003 and the Critical Infrastructure Information Subtitle of the Homeland Security Act of 2002*, *at* http://leahy.senate.gov/press/200303/031203a.html (last visited Oct. 20, 2003) (on file with the American University Law Review).

291. S. 609, 108th Cong. § 2 (2003).

292. *See generally id.*

293. *See* Clinton Memorandum, *supra* note 52 (arguing that because citizens in a democratic government must have access to information, agencies should renew their commitment to FOIA, an important means by which to disseminate information).

294. *See* Statement of Leahy, *supra* note 89, at S11423 (explaining that current FOIA exemptions balance public safety and national security with open disclosure of government information).

are entitled to most of the information they seek.[295] With the broad new CIIA FOIA exemption and a DOJ that will vigorously defend almost all agency FOIA decisions, the time period for responding to the requesting public could expand greatly, especially in light of preexisting backlogs and the amount of time it could take for administrative appeals and further litigation.

The significance of September 11, 2001 and its impact on the freedom of information cannot be ignored—it has affected the perception of privacy, congressional lawmaking, and perhaps even court decisions.[296] But this does not justify the expansion of governmental secrecy post-September 11, 2001.[297] One would be hard-pressed to find a spokesperson for the notion that even sensitive information should flow unimpeded to the public in the name of governmental transparency.[298] We all want to keep our country secure and our people safe, but the exemption framework codified at 5 U.S.C. § 552 protects adequately against the release of sensitive data that could place the U.S. at risk.[299]

---

295. *See* GAO, *supra* note 22, at 57 (discussing the potential "chilling effect" of the FOIA policy change under the Bush Administration); *see also* Statement of Swire, *supra* note 89 (arguing that the DHS FOIA provision should have been deleted from the Act because the provision permits the DHS to secret information it receives, even if the information is otherwise available through FOIA requests).

296. *See generally* Rotenberg, *supra* note 9, at 1115 (examining the relationship between privacy and secrecy and the events of September 11, 2001). After the horrific events of September 11, 2001, "[r]egulation changes that most would have opposed or thought impractical and overbearing before September 11 will be welcomed." Vartanian, *supra* note 101, at *2; *see also* Robin Toner, *Some Foresee A Sea Change In Attitudes On Freedoms*, N.Y. TIMES, Sept. 15, 2001 (discussing congressional attitudes towards civil liberties in the wake of the September 11 tragedy), *available at* http://www.nytimes.com/2001/09/15/national/15CIVI.html (on file with the American University Law Review). *But see* Beierle & Bell, *supra* note 135 (citing a N.Y. TIMES/CBS poll from December 2001 demonstrating public concern that FOIA will impede on core civil liberties).

297. *See* Rotenberg, *supra* note 9, at 1123-25 (arguing that the expansion in government secrecy post-September 11, 2001 appears to be growing unimpeded with the enactment of the USA PATRIOT Act (Pub. L. No. 107-56) and closed hearings, in conjunction with limited access to public records under FOIA).

298. *See* Tapscott, *supra* note 64 (asserting that although the Bush Administration's efforts address legitimate national security issues in the war against terrorism, no one has produced an example of sensitive information that could not have been exempted from disclosure under FOIA's preexisting statutory exemptions); *see also* Parker, *supra* note 3 (arguing that withholding information about certain sensitive infrastructure sectors, including nuclear power plants, pipeline routes, chemical supplies, and the airlines seems appropriate for national security purposes).

299. *See* Statement of Leahy, *supra* note 89, at S11423 (arguing that encouraging information sharing between the public and private sectors is a laudable goal supported by Congress but that the FOIA exemption provided by the CIIA is an inappropriate way to meet this goal).

Those who believe that the overly broad cession of the public's right to know is necessary in this "war against terrorism"[300] should recall the remarks of a certain Republican congressman from Illinois:

> [D]isclosure of government information is particularly important today because government is becoming involved in more and more aspects of every citizen's personal and business life, and so access to information about how government is exercising its trust becomes increasingly important.[301]

Donald Rumsfeld made this statement in support of FOIA in turbulent 1966. Now the Bush Administration's Secretary of Defense, Secretary Rumsfeld's words ring true in this era of increased government secrecy, when governmental transparency appears to have become a casualty of war.[302] Only time will reveal the effects of these new restrictions on the public's right to government information. As long as the Bush Administration and Congress refuse to work within the adequate preexisting FOIA framework to address national security concerns, the prospects for governmental transparency in this new era appear grim.

300. *See* Tapscott, *supra* note 64 (reporting surveys indicating that Americans may be willing to trade civil liberties for security against terrorism). *But see* Parker, *supra* note 3 (decrying congressional silence in light of the Bush Administration's secrecy efforts and reporting that critics argue that the Administration's clampdown on disclosure is opportunistic).

301. Tapscott, *supra* note 64.

302. *See* Beierle & Bell, *supra* note 135.