Harvard Journal of Law & Technology
Volume 15, Number 2 Spring 2002

DISCLOSURE OF GOVERNMENT INFORMATION ONLINE: A NEW APPROACH FROM AN EXISTING FRAMEWORK

Paul M. Schoenhard[*]

TABLE OF CONTENTS

I. INTRODUCTION

Within hours of the September 11 attacks, United States government ("Government") web content started disappearing from the Internet. In the days and weeks that followed, the Executive Branch

* J.D. 2003 (expected), Harvard Law School. The Author would like to thank Professor Jonathan Zittrain for his advice and Amy Ligler for her loving support.

clamped down on information at all levels and redefined the requirements and expectations of Government secrecy. Now, as Congress and the Executive Branch move forward, we must decide if these changes are necessary, or permissible.

This Note will address the delicate balance between public awareness and national security on the Internet, a balance that needs to be maintained even in times of crisis and national emergency. Parts II and III will provide the legal framework and motivation for the arguments in Parts IV through VI. Part II will discuss the status quo prior to the events of September 11: statutory requirements of Government disclosure on the Internet, their Executive interpretations, and popular consensus. Part III will establish the new status quo and existing proposals for further change. Part IV will argue that the Executive Branch's post-September 11 response effectively ignored the requirements of the Freedom of Information Act ("FOIA"). Part V will argue that Government disclosure via the Internet is necessary and that our existing legal framework is functional even in times of crisis. Part VI will apply the conclusions of Parts IV and V to two brief case studies: web pages pulled from the Internet by the Department of Transportation ("DOT") and by the Environmental Protection Agency ("EPA") after September 11. This Note will conclude by arguing that the FOIA requires the Government to continuously offer electronic access to information once it is made available online.

II. THE STATUS QUO

A. Background

The notion that information should be readily available to the public can be traced back to our founding fathers. James Madison wrote, "A popular government without popular information, or the means of acquiring it, is but a prologue to a farce or a tragedy, or perhaps both . . . a people which mean to be their own governors must arm themselves with the power which knowledge gives."[1] As our society has evolved, so has the application of this idea.

Prior to the passage of the FOIA, the prevailing public access law was Section 3 of the Administrative Procedure Act of 1946 ("APA").[2] This section was interpreted to *limit* the amount of information the Government needed to disclose to the public. In 1955, the House Committee on Government Operations established the Special Subcommittee on Government Information. This subcommittee produced

1. Letter from James Madison, to W.T. Barry (Aug. 4, 1822) *in* 9 THE WRITING OF JAMES MADISON 103 (Gaillard Hunt ed., 1910).

2. Pub. L. No. 79-404, 60 Stat. 237 (1946) (codified in scattered sections of 5 U.S.C.).

a 1958 amendment to the APA which stated that it "does not authorize withholding information from the public or limiting the availability of records to the public."[3] This trend towards openness continued. In 1966, Congress passed the FOIA as an amendment to the APA. Upon signing the FOIA, President Lyndon Johnson stated, "This 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."[4]

The FOIA requires agency disclosure of documents in three ways. First, agencies must publish agency contact information, "statements of the general course . . . by which its functions are channeled and determined," procedural requirements, and "substantive rules of general applicability . . . and statement of general policy" in the Federal Register.[5] Second, additional information must be placed in Government reading rooms:[6] final opinions and orders, statements of policy not published in the Federal Register, and administrative staff manuals and instructions.[7] Third, the public can use a mechanism, established by the FOIA, to request any non-exempt document directly from a Federal agency (a "FOIA request").[8] The FOIA authorizes nine exemptions, including national security information, solely internal documents, information exempted by statute, and some personal information.[9]

Over the next thirty years, application of the FOIA significantly modified Government behavior, uncovering everything in Congress's own estimation from Government waste and fraud to consumer health dangers.[10] Despite these benefits to society, federal agencies soon felt the burden of backlogged FOIA requests, demanding time and re-

---

3. Pub. L. No. 85-619, 72 Stat. 547 (1958) (codified as amended at 5 U.S.C. § 301 (2001)).

4. H. REP. NO. 104-795, at 8 (1996).

5. 5 U.S.C. § 552(a)(1) (2001).

6. "Reading rooms" is a general term for repositories in which Government records are available for public inspection. *See* U.S. Dep't of Justice, *FOIA Reading Rooms*, FREEDOM OF INFORMATION ACT GUIDE (May 2000), *available at* http://www.usdoj.gov/oip/readingroom.htm. Although the layout and security procedures of Government reading rooms are not statutorily established, records under FOIA subsection (a)(2) must be made "available for public inspection; no demand is necessary." Jordan v. U.S. Dep't of Justice, 591 F.2d 753, 756 (D.C. Cir. 1978).

7. 5 U.S.C. § 552(a)(2) (2001). The Electronic Freedom of Information Amendments added categories of information that the Government is required to disclose in this manner. These provisions will be discussed in Part II(b), *infra*.

8. 5 U.S.C. § 552(a)(3) (2001).

9. 5 U.S.C. § 552(b) (2001).

10. *See* Electronic Freedom of Information Amendments of 1996, Pub. L. No. 104-231, 110 Stat. 3048 (codified at 5 U.S.C. § 552 (2001)) ("[T]he Freedom of Information Act has led to the disclosure of waste, fraud, abuse, and wrongdoing in the Federal Government; . . . [T]he Freedom of Information Act has led to the identification of unsafe consumer products, harmful drugs, and serious health hazards.").

sources the agencies lacked.[11] The 1990s ushered in a new era of technological advancement, referred to as the "Information Age,"[12] during which the public and Government first benefited from the Internet. Federal departments and agencies took advantage of these new opportunities to disseminate information at low cost.[13]

Meanwhile, the Clinton Administration embarked on a campaign to release unprecedented quantities of information to the public. On October 4, 1993, President Clinton circulated a memo expressing the Administration's commitment to the FOIA: "Each agency has a responsibility to distribute information on its own initiative, and to enhance public access through the use of electronic information systems. Taking these steps will ensure compliance with both the letter and spirit of the Act."[14] Thus, prior to any explicit statutory language, President Clinton instructed federal agencies to view the FOIA as requiring that Government information be available online. Attorney General Janet Reno, in accordance with this sentiment, circulated a memo as an attachment to the President's, informing all federal agencies that the Department of Justice ("DOJ"), "in determining whether or not to defend a nondisclosure decision . . . will apply a presumption of disclosure."[15] Under this presumption, agencies were required to disclose information unless it was absolutely necessary not to do so.[16] According to the Attorney General, "this change in policy serves the public interest by achieving the Act's primary objective — maximum responsible disclosure of government information — while preserving essential confidentiality."[17] Then, in 1995, President Clinton filed an Executive Order[18] revoking the classification schemes established

---

11. As of 1996, the FBI reportedly had a FOIA backlog of up to four years. *See* 142 CONG. REC. S10,893–94, S10,893 (daily ed. Sept. 18, 1996) (statement of Sen. Leahy) [hereinafter Leahy]; *see also* H.R. REP. NO. 104-795, at 6 (1996), *reprinted in* 1996 U.S.C.C.A.N. 3449 ("At some agencies failure to allocate sufficient staff to comply with the Act has resulted in lengthy backlogs measured in years.").

12. *See, e.g.*, David M. Anderson, *America Has No Name for Its New Age*, PLAIN DEALER (Cleveland), Oct. 17, 2001, at B13.

13. More than 800 Federal websites were established between 1993 and 1996. *See* H.R. REP. NO. 104-795, at 12 (citing Lisa Corbin, *Cyberocracy*, GOV'T EXECUTIVE, Jan. 1996, at 28).

14. Memorandum from President William J. Clinton on The Freedom of Information Act, to the Heads of Departments and Agencies (Oct. 4, 1993).

15. Memorandum from Attorney General Janet Reno on The Freedom of Information Act, to Heads of Departments and Agencies (Oct. 4, 1993).

16. *Id.* ("[The exemptions to the FOIA] are best applied with *specific reference* to such harm [to Government and private interests], and only after consideration of the reasonably expected consequences of disclosure in each particular case. . . . Where 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.").

17. *Id.*

18. Exec. Order No. 12,958, 60 Fed. Reg. 19,825 (Apr. 17, 1995).

during the Reagan Administration[19] for a more open-disclosure policy. Responding to these shifts in Executive policy and the dawn of the Information Age, Congress worked to update the FOIA.

B. EFOIA and the Disclosure of Government Information Online

After a number of failed legislative attempts,[20] Congress passed the Electronic Freedom of Information Amendments ("EFOIA")[21] in 1996. Although much of EFOIA is directed to alleviating agency backlogs,[22] the act also requires the electronic availability of many Government records, inserting the following amendments into section 552(a)(2):

> (D) copies of all records, regardless of form or format, which have been released to any person under paragraph (3) and which, because of the nature of their subject matter, the agency determines have become or are likely to become the subject of subsequent requests for substantially the same records; and
> (E) a general index of the records referred to under subparagraph (D);
> . . . For records created on or after November 1, 1996, within one year after such date, each agency shall make such records available, including by computer telecommunications.[23]

In effect, these provisions required federal agencies to establish "electronic reading rooms" — counterparts to traditional FOIA reading rooms. Electronic reading rooms must contain all agency records produced in electronic format after November 1, 1996 that would ordinarily be placed exclusively in paper FOIA reading rooms. Under subparagraph (D), EFOIA also requires electronic and traditional reading rooms to contain materials that have been or are likely to be subjects of multiple FOIA requests.

---

19. Exec. Order No. 12,356, 47 Fed. Reg. 14,874 (Apr. 6, 1982) (revoked by Exec. Order No. 12,958, Fed. Reg. 19,825 (Apr. 17, 1995)).

20. *See* H.R. REP. NO. 104-795, at 6 (1996), *reprinted in* 1996 U.S.C.C.A.N. 3449.

21. Electronic Freedom of Information Amendments of 1996, Pub. L. No. 104-231, 110 Stat. 3048 (codified at 5 U.S.C. § 552 (2001)).

22. *See id.* at 3050–52; Leahy, *supra* note 11, at S10,894 ("[T]he bill would address the biggest single complaint of people making FOIA requests: delays in getting a response.").

23. EFOIA, 110 Stat. at 3049.

Additionally, EFOIA was intended to encourage agencies to maintain informative websites.[24] Many executive agencies did just that. Government websites flourished on the Internet,[25] providing information to members of the public who would otherwise be unable to access paper reading rooms and for whom FOIA requests would be impractical.

This environment of openness continued until September 11, 2001.[26]

III. THE NEW ENVIRONMENT

A. The Information Clampdown

> For better or worse . . . the easy availability of information about myriad government activities is one facet of American society that may have been forever changed by September 11.[27]

As a result of the Government's information clampdown, content once part of the public domain is no longer available; its return to the public domain is uncertain if not doubtful. The removed websites include the DOT's National Pipeline Mapping System and the EPA's pages of Risk Management Plans.[28] Other pages to disappear included information from the Department of Energy[29] and the Nuclear Regula-

---

24. *See id.* at 3048 ("Government agencies should use new technology to enhance public access to agency records and information."); H.R. REP. NO. 104-795, at 11 ("An underlying goal of H.R. 3802 is to encourage on-line access to Government information available under the FOIA, including requests ordinarily made pursuant to section 552(a)(3). As a result, the public can more directly obtain and use government information.").

25. In 2000, the General Accounting Office conducted an evaluation of twenty-five agencies' EFOIA implementations. The results can be found in U.S. General Accounting Office, INFORMATION MANAGEMENT: PROGRESS IN IMPLEMENTING THE 1996 ELECTRONIC FREEDOM OF INFORMATION ACT AMENDMENTS (Mar. 2001), *available at* http://www.gao.gov/new.items/d01378.pdf (last visited Mar. 1, 2002).

26. According to Department of Defense spokesman Glenn Flood, "Everything is sort of a little different than before Sept. 11." Jim Wolf, *Secrecy Foe Joins U.S. Move to Scrub Data on Web*, Reuters, Oct. 11, 2001, *available at* http://www.fas.org/sgp/news/2001/10/re101101.htm (last visited Mar. 1, 2002).

27. Toby Eckert, *Federal Agencies Pull Data from Web Sites After Sept. 11*, SAN DIEGO UNION-TRIB., Dec. 9, 2001, at A13.

28. The Government's handling of information previously available on these web pages will be discussed further in *infra* Part VI.

29. On the advice of the Project on Government Oversight, the Department of Energy removed pages that provided details on nuclear energy facilities. *See* Joshua Dean, *Energy Pulls Sensitive Nuclear Information from the Web*, *at* http://www.govexec.com/dailyfed/1101/111201j1.html (Nov. 12, 2001).

tory Commission.[30] Much of the information that was removed from the Internet may still be available through traditional FOIA requests,[31] but in some cases, the information has been restricted to only certain requesters.[32] Although this Note will primarily address this sudden and dramatic change in online information disclosure by the Government, it is useful to review the other aspects of the Executive Branch's information clampdown in the wake of September 11.

On September 14, 2001, President George W. Bush declared a national emergency,[33] thereby assuming the executive powers granted under the National Emergency Act.[34] Acting in his role as Commander-in-Chief, the President called up the armed services,[35] instituted military tribunals,[36] and shrouded the Executive Branch in secrecy. Responding to national consensus that civil liberties should not be casualties of the war on terrorism,[37] President Bush stated, "We're an open society, but we're at war. . . . Foreign terrorists and agents must never again be allowed to use our freedoms against us."[38] Attorney General John Ashcroft and Deputy Defense Secretary Paul Wolfowitz followed suit.

On October 12, 2001, Ashcroft released a memo reinterpreting the FOIA for the new Administration (the "Ashcroft memo").[39] The Ashcroft memo marks a dramatic shift from the policies espoused in the Reno memo. Because of its potential for abuse, the Ashcroft memo warrants quotation at some length:

---

30. According to OMB Watch, the NRC "completely shut down its web site, and more recently restored 'select content.'" *See The Post-September 11 Environment: Access to Government Information, at* http://www.ombwatch.org/info/2001/access.html (last visited Jan. 20, 2002) (listing many of the websites removed in the wake of Sept. 11).

31. David Corn, *Nation of Poisons*, AMICUS J., Jan. 1, 2002, at 24.

32. *See infra* Part VI(a) (discussing information access restrictions imposed by the Department of Transportation).

33. Proclamation No. 7463, 66 Fed. Reg. 48,199 (Sept. 14, 2001) ("[P]ursuant to the National Emergencies Act (50 U.S.C. 1601 et seq.), I intend to utilize the following statutes: sections 123, 123a, 527, 2201(c), 12006, and 12302 of title 10, United States Code, and sections 331, 359, and 367 of title 14, United States Code.").

34. 50 U.S.C. § 1601 et seq. (2002).

35. Exec. Order No. 13,223, 66 Fed. Reg. 48,201 (Sept. 14, 2001).

36. Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terror, 66 Fed. Reg. 57,833 (Nov. 13, 2001).

37. *See infra* note 114 and accompanying text.

38. Brad Knickerbocker, *Security Concerns Drive Rise in Secrecy*, CHRISTIAN SCI. MONITOR, Dec. 3, 2001, at 1 (quoting President George W. Bush).

39. Memorandum from John Ashcroft, Attorney General, to the Heads of all Federal Departments and Agencies (Oct. 12, 2001). It is customary for the Attorney General of each presidential administration to circulate a general statement of policy regarding the FOIA. It is unclear whether Attorney General John Ashcroft's memo of October 12 will be the Bush Administration's general policy or merely a temporary reaction to Sept. 11. Only time will tell.

> It is only through a well-informed citizenry that the leaders of our nation remain accountable to the governed and the American people can be assured that neither fraud nor government waste is concealed.
> The Department of Justice and this Administration are equally committed to protecting other fundamental values that are held by our society. Among them are safeguarding our national security, enhancing the effectiveness of our law enforcement agencies, protecting sensitive business information and, not least, preserving personal privacy. . . .
> Any discretionary decision by your agency to disclose information protected under the FOIA should be made only after full and deliberate consideration of the institutional, commercial, and personal privacy interests that could be implicated by disclosure of the information. . . .
> When you carefully consider FOIA requests and decide to withhold records, in whole or in part, you can be assured 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.[40]

The first two sentences of the Ashcroft memo are an odd and poignant juxtaposition. In this statement, Ashcroft establishes the concepts of Government transparency and freedom as mutually exclusive goals of his Department. Thus interpreted, the FOIA becomes more of a balancing act than a statutory mandate. Unlike the Reno memo, which declared a presumption of full disclosure, the Ashcroft memo instructs agencies to make "full and deliberate consideration" prior to disclosure of information and to "carefully consider FOIA requests." 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. The obvious catch-22 of (b) aside,[41] the Ashcroft memo seriously under-

40. *Id.*

41. By stating that the DOJ will not defend an agency's decision to withhold agency records if that decision jeopardizes another agency's ability to do the same, Ashcroft implies that the DOJ retains the power to prioritize classification of Government information — a universal power not traditionally held by the Department.

mines the ability of the public to utilize the tools offered by the FOIA.[42]

The Department of Defense ("DOD") also clamped down on information access. On October 18, 2001, Deputy Defense Secretary Paul Wolfowitz circulated a similar memorandum within the DOD (the "Wolfowitz memo"),[43] which stated:

> [I]t is clear that . . . the security of information critical to the national security will remain at risk for an indefinite period.
>
> It is therefore vital that Defense Department employees, as well as persons in other organizations that support DOD, exercise *great* caution in discussing information related to DOD work, regardless of their duties. Do not conduct *any* work-related conversations in common areas, public places, while commuting, or over unsecured electronic circuits. Classified information may be discussed *only* in authorized spaces and with persons having a specific need to know and the proper security clearance. Unclassified information may likewise require protection because it can often be compiled to reveal sensitive conclusions. Much of the information we use to conduct DOD's operations must be withheld from public release because of its sensitivity. If in doubt, do not release or discuss official information except with other DOD personnel. . . .
>
> We must ensure that we deny our adversaries the information essential for them to plan, prepare or conduct further terrorist or related hostile operations against the United States and this Department.[44]

---

42. *See* Tom Beierle & Ruth Greenspan Bell, *Don't Let 'Right to Know' Be a War Casualty*, CHRISTIAN SCI. MONITOR, Dec. 20, 2001, at 9 ("Years of hard-won battles that turned FOIA into a fundamental routine bulwark against government secrecy were undermined in a day. The memo ushered out the principle of 'right to know' and replaced it with 'need to know.' Now, the presumption is that information is inherently risky.").

43. Memorandum from Paul Wolfowitz, Deputy Defense Secretary, to the DOD (Oct. 18, 2001), *available at* http://www.fas.org/sgp/news/2001/10/wolfowitz.html (last visited Mar. 1, 2002). The Wolfowitz memo is discussed in the context of Army websites in Hampton Stephens, *Security Concerns Prompt Army to Review Web Sites, Access*, DEFENSE INFORMATION AND ELECTRONICS REPORT, Oct. 26, 2001, *available at* http://www.fas. org/sgp/news/2001/10/dier102601.html (last visited Mar. 1, 2002).

44. Wolfowitz, *supra* note 43 (emphasis in original).

Early in the memo, Wolfowitz states that "the security of information critical to the national security will remain at risk for an *indefinite* period."[45] Just as with the Ashcroft memo and the removals of many agency websites, there is no sunset provision in Wolfowitz's directive, nor one in the Executive Branch's clampdown as a whole. Then, against the grain of the FOIA and the United States's general conception of a "right-to-know," Wolfowitz instructs that "[u]nclassified information may likewise require protection because it can often be compiled to reveal sensitive conclusions."[46] This concept is known as the "mosaic approach," an argument derived "from the executive order, which defines 'classified' information as that which, if disclosed, would cause damage 'either by itself or in the context of other information.'"[47] Although this logic is reasonable, it fails to note Congress's express instruction in the FOIA that only information specifically exempted from disclosure as national security information by executive determination may be withheld from the public. Instead, a logical conclusion drawn from the Wolfowitz memo is that the DOD no longer needs to disclose *any* information to the public.

Finally, Wolfowitz concludes with a sentiment similar to that expressed by the President: "We must ensure that we deny our adversaries the information essential for them to plan, prepare or conduct further terrorist or related hostile operations against the United States and this Department."[48] This stalwart expression of the Executive Branch's resolve to protect our nation by limiting the public's access to information is illustrative of the new status quo. Yet, we must step back, assess what has transpired, and choose a path for the future.

B. Proposals for the Future

The Executive and Legislative branches both already have begun contemplating new policies and statutes. Some of the proposals on the table have been considered and have taken on new significance. Others are new ideas for the present climate of perceived vulnerability and insecurity. Congress is now reviewing potential amendments to the FOIA,[49] an Energy Security Bill,[50] and a number of more minor

45. *Id.* (emphasis added).

46. *Id.*

47. Robert P. Deyling, *Judicial Deference and De Novo Review in Litigation over National Security Information Under the Freedom of Information Act*, 37 VILL. L. REV. 67, 84 (1992).

48. Wolfowitz, *supra* note 43.

49. William Jackson, *Clark Unveils Security Strategies*, GOV'T COMPUTER NEWS, Dec. 10, 2001, *available at* http://www.gcn.com/20_34/news/17620-2.html (last visited Mar. 1, 2002) ("[Presidential cybersecurity adviser Richard A.] Clarke also said President Bush supports a bill introduced by Sen. Robert Bennett (R-Utah) to

resolutions directed to information security. It has focused on legislation intending to clarify the Executive Branch's information disclosure requirements. The Executive Branch's ideas vary from the simple — agency review of website content — to the complex — the creation of a large secure Government intranet. These proposals largely ignore the FOIA, instead seeking new legal regimes to shape the future of Government information disclosure.

Although no official order has been published in the Federal Register,[51] federal agencies have started reviewing their web postings, past and present.[52] President Bush, meanwhile, has published an Executive Order[53] directing the Secretary of Defense and the Director of Central Intelligence to prepare guidelines for the protection of national security information on the Government's information systems.[54] Although a narrow reading of this order would grant authority merely to protect the systems containing national security information, a broader reading indicates a grant of authority to rein in even further potentially sensitive Government information.

A more large-scale Executive Branch proposal is the creation of a secure Government intranet, known as GovNet. GovNet would become the Government's central repository for information, offering access to all documents according to varying levels of security classifications. The GovNet concept has been criticized by right-to-know activists who worry that documents would no longer be posted directly to the Internet for public access.[55] If, as discussed earlier, all

---

amend the Freedom of Information Act to protect information shared by companies with the government.")

50. Corn, *supra* note 31 ("Senator Jeff Bingaman (D-N.M.) circulated a draft energy security bill that would have severely restricted government's need to respond to FOIA requests.").

51. As of January 25, 2002, searches of the Federal Register's database and the White House's press releases did not reveal any pertinent orders published since September 11.

52. *See* Eckert, *supra* note 27.

53. Exec. Order No. 13,231, 66 Fed. Reg. 53,063 (Oct. 16, 2001).

54. *Id.* ("In consultation with the Assistant to the President for National Security Affairs and the affected departments and agencies, the Secretary of Defense and the DCI [Director of Central Intelligence] shall develop policies, principles, standards, and guidelines for the security of national security information systems that support the operations of other executive branch departments and agencies with national security information.").

55. *See* William Jackson, *GovNet Ideas Don't Come Cheaply*, GOV'T COMPUTER NEWS, Dec. 10, 2001, at 9.

> Doing GovNet right means maintaining "delicate balance" between security and public access to information, Center for Democracy & Technology (CDT) Assoc. Dir. Ari Schwartz said. . . . CDT is concerned about GovNet as proposed . . . because it wasn't clear how it [GovNet] would ensure access to public information, given that system for obtaining govt. information (un-

agency information except that which falls within the specified exemptions should be open to the public, such a large-scale effort should be unnecessary.

These proposals have the potential to drastically limit the amount of information traditionally available to the public, under the faulty assumption that the current security threat requires a new legal or organizational regime. The following Part will address this faulty assumption and explain how existing law — the FOIA — applies to Government information online.

IV. DISCUSSION

A. The New Playing Field Is Not So New

September 11 dramatically changed the outlook of the American government and people. In the nation's time of need and shock, the Bush Administration's strong positions were understandable. Addressing a Joint Session of Congress, a somber President Bush declared, "Tonight we are a country awakened to danger and called to defend freedom. Our grief has turned to anger, and anger to resolution."[56]

This resolution, similar to that of past Presidents facing conflicts, will serve the country well in wartime but brings with it the danger of sacrificing the very freedoms we seek to protect. 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.[57] Although President Bush repeatedly has pledged his sup-

---

> der the electronic Freedom of Information Act) doesn't work all that well now.

Id.

56. President George W. Bush, Address to a Joint Session of Congress and the American People (Sept. 20, 2001), *available at* http://www.whitehouse.gov/news/releases/2001/09/20010920-8.html (last visited Mar. 1, 2002).

57. *See* 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 ("During the Civil War, Abraham Lincoln suspended the right of habeas corpus, the constitutionally enshrined procedure by which a defendant can challenge a wrongful conviction. In World War II, Franklin Roosevelt interned 120,000 Japanese Americans and tried accused German saboteurs in military courts."); Center for Democracy & Technology, Preserving Democratic Freedoms in Times of Peril, *at* http:/www.cdt.org/security/010914cdtstatement.shtml (Sep. 14, 2001) ("History teaches us that when we sacrifice liberty in times of crisis we later come to regret it, from the Alien Sedition Act to the internment of Japanese Americans to the FBI surveillance of anti-Vietnam war demonstrators and civil rights leaders.").

port for America's freedoms,[58] the President's statement, "We're an open society, but we're at war"[59] may indicate a problematic tendency.

We should carefully note this tendency's potential ramifications on the future of Government information disclosure on the Internet. The Executive Branch's mass removal of such information sets a precedent for future administrations and undermines the public's right-to-know. The disappearance of Government websites in the wake of September 11 constitutes the first Government-wide removal of information from the Internet. Just as the Executive relies on existing legal regimes to empower himself as Commander-in-Chief, we must not, even in the face of new threats, assume away the ability of the FOIA both to preserve the people's right-to-know and to protect the national security. When agency websites started disappearing from the Internet, the American public lost a great deal more than a few ordinary web pages. Unfortunately, the courts have not yet had occasion to deal with the removal of Government information from the Internet. Without explicit statutory authority or legal precedent, the Executive Branch has seized the opportunity to remove information.

B. The FOIA Prohibits the Removal of Government Web Content

As a statutory regime, the FOIA has responded well to the information needs of the American public. It is surprising, then, that the FOIA has not been applied to Government web content. Although such an application was perhaps unnecessary when web content remained available online, examination of the FOIA indicates that the FOIA *does* protect the public's right-to-know with respect even to web pages. Because this application is not explicit in the legislative history of the FOIA or EFOIA and has not been tested by the courts, we must work from the bottom up.

Under the Freedom of Information Act, the definition of "record" is critical to the present debate. If web pages are not records, then the Government may remove web content from the public domain at will and with impunity. The FOIA definition is rather vague: "'record' and any other term used in this section in reference to information includes any information that would be an agency record subject to the requirements of this section when maintained by an agency in any format, including an electronic format."[60] Under this definition, a web

58. *See* President George W. Bush, Address to the Nation (Sept. 11, 2001) ("[W]e go forward to defend freedom and all that is good and just in our world."); President George W. Bush, Remarks at National Day of Prayer and Remembrance (Sept. 14, 2001) ("[W]e are freedom's home and defender. And the commitment of our fathers is now the calling of our time.").

59. Knickerbocker, *supra* note 38, at 1.

60. 5 U.S.C. § 552(f)(2).

page is also a "record." It is a collection of information in a tangible form and stored in a medium (a web server). Web pages containing information on agency policies, programs, personnel, etc., are thus records for purposes of the FOIA.

The legislative history of EFOIA lends further credence to this argument. The final House Committee report comments on the meaning of the term "record":

> [A] "record" under the FOIA includes electronically stored information. This articulates the existing general policy under the FOIA that all Government records are subject to the Act, regardless of the form in which they are stored by the agency. . . .
> The format in which data is maintained is not relevant under the FOIA. Computer tapes, computer disks, CD-ROMs, and all other digital or electronic media are records. Microfiche and microforms are records. When other, yet-to-be invented technologies are developed to store, maintain, produce, or otherwise record information, these will be records as well. When determining whether information is subject to the FOIA, the form or format in which it is maintained is not relevant to the decision. . . .
> The primary focus should always be on whether information is subject to disclosure or is exempt, rather than the form or format it is stored in.[61]

This lengthy statement deserves some parsing. A web page is "electronically stored information" and thus a record. Because "all government records are subject to the Act," Government web pages must be available to the public under the FOIA. The committee report proceeds to itemize acceptable formats, leaving room for "all other digital or electronic media." Records also include technologies that "store, maintain, produce, or otherwise record information." Both of these latter descriptions certainly would include web pages in the definition of 'records.' Finally, the Committee falls back on a more general principle: "whether information is subject to disclosure or exempt." This final statement indicates that *all* Government information not specifically exempted from disclosure under the FOIA is subject to disclosure.

The courts have also contributed to this debate. In *Essential Information, Inc. v. United States Information Agency*,[62] the appellate court was asked to determine whether web addresses constitute re-

61. H.R. REP. NO. 104-795, *supra* note 20.
62. 134 F.3d 1165, 1166 (D.C. Cir. 1998).

cords for purposes of the FOIA. The court declined to reach this issue but agreed with the district court's decision that web addresses are a "means to access records."[63] The natural corollary to this determination is that web pages — the objects accessed by web addresses — may be records. More generally, the Supreme Court has considered the definition of "record" extensively in *Kissinger v. Reporters Committee for Freedom of the Press*,[64] *Forsham v. Harris*,[65] and *United States Department of Justice v. Tax Analysts*.[66] In this trio of opinions, the Court established a two-prong test for agency records: whether (1) the material has been created or obtained by the agency; and (2) the agency is in control of the material.[67] Surely, material posted to agency websites is under the control of the posting agency, and material that has been posted must first be either created or obtained by the agency. Although the Supreme Court's opinions on this subject do not address the Internet, the basic requirements of an "agency record" are met by Government web pages.

Outside the FOIA context, the appellate court in *Armstrong v. Executive Office of the President*[68] considered the definition of "record" for purposes of the Federal Records Act, citing a definition that would embrace web pages: "'[r]ecords' are defined by the [Federal Records Act] as documentary materials 'made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business.'"[69] Government web pages fit this definition: they are "documentary materials" generated "in connection with the transaction of public business." Although this definition of "record" is not dispositive with regard to the FOIA, it would tend to further indicate that Government web pages should fit into the category of Government records. Having established that Government web pages are "records" under the FOIA, we must next consider the FOIA's disclosure requirements with respect to web pages. This is answered more simply than the definitional question above. In *Schladetsch v. United States Department of Housing and Urban Development*,[70] the court determined that, "The FOIA applies equally to all agency records, regardless of format. 'Although accessing information from computers may involve a somewhat different process than locating and retrieving manually-stored records, these differences may not be used to circumvent the full disclosure policies of the

63. *Id.* at 1166 n.3.
64. 445 U.S. 136 (1980).
65. 445 U.S. 169 (1980).
66. 492 U.S. 136 (1989).
67. *Id.* at 144–45.
68. 90 F.3d 553, 557 (D.C. Cir. 1996).
69. *Id.* (citing 44 U.S.C. § 3301 (1976)).
70. No. 99-0175, 2000 W.L. 33372125, at *1 (D.C. D. Apr. 4, 2000).

FOIA.'"[71] This holding is consistent with the House Committee report's statement that "[w]hen determining whether information is subject to the FOIA, the form or format in which it is maintained is not relevant to the decision."[72] The disclosure requirements of the FOIA, and by inclusion EFOIA, thus apply to Government web pages just as they do other Government documents.

Nonetheless, agencies are claiming exemptions, often without meeting the statutory requirements for such exemptions. As discussed above, the FOIA requires disclosure upon request of *all* Government records, except those specifically exempted by one of the nine FOIA exemptions. The reported reason for the disappearance of Government web pages after the events of September 11 is national security. Exemption 1 of the FOIA (the "national security exemption") provides for just this, exempting information that is "(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) [is] in fact properly classified pursuant to such Executive order."[73] Agencies claiming the national security exemption in this manner, however, would fail on two counts: (1) the national security exemption requires a *specific* reason for classification; and (2) the national security exemption does not apply to information already in the public domain.

The courts have the power to review agency classification determinations[74] and regularly do so. The 1974 Amendments to the FOIA explicitly gave the courts the power to review documents exempt for reasons of national security in camera.[75] Afterward, the courts have wielded this authority to review agency classification decisions, inspecting even documents withheld in "good faith."[76]

---

71. *Id.* at *3 (citing Yeager v. DEA, 678 F.2d 315, 321 (D.C. Cir. 1982)).

72. H.R. REP. NO. 104-795, *supra* note 4.

73. 5 U.S.C. § 552(b)(1).

74. Under the FOIA, district courts are granted "jurisdiction to enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld from the complainant"; and the power to "determine the matter de novo" with "the burden . . . on the agency to sustain its action." 5 U.S.C. § 552(a)(4)(B).

75. Act of November 21, 1974, Pub. L. No. 93-502, 1974 U.S.C.C.A.N (88 Stat. 1561) (codified at 5 U.S.C. § 552(a)(4)(B)).

76. *See* Ray v. Turner, 587 F.2d 1187 (D.C. Cir. 1978).

> Congress feared more than 'bad faith' in the exercise of agency discretion to withhold government information. Even 'good faith' interpretations by an agency are likely to suffer from the bias of the agency, particularly when the agency is as zealous as the CIA has been in its responsibility to protect 'national security.' Being aware of the dangers of relying too much on agency 'expertise,' Congress required the courts to take a fresh look at decisions against disclosure as a check against both intentional misrepresentations and inherent biases.

Id. at 1210 (Skelly Wright, C.J., concurring) (footnote omitted).

If an agency properly classifies a document pursuant to an Executive Order, there is an almost unrebuttable presumption that the record is properly withheld under the national security exemption. The courts have not questioned the President's ability to determine which categories of information should or should not be classified, leaving the President almost unlimited power. The Supreme Court in *Department of the Navy v. Egan*[77] held that the President's power to classify information derives directly from the Constitution without Congressional mandate.[78] Once classified, a document remains classified as long as the controlling agency believes that the information poses a security risk.[79]

In the present situation, however, there is no statutory or Executive basis for the classification of information previously available on the Internet. No Executive Orders have been issued offering classification guidance.[80] Attorney General John Ashcroft's guidance is too vague to base classification upon.[81] As a result, unless information previously on Government web pages *should have been* classified originally, there is no basis for them to be classified and withheld under the national security exemption now.

Even if Government web pages that have been pulled off the Internet are now properly classified, the Government must still make them available for FOIA requests. Once information has been disclosed to the public, such information can no longer be withheld under an exemption. In *Founding Church of Scientology v. NSA*,[82] the Court held that suppression of "well publicized" information would frustrate the aims of the FOIA without advancing countervailing in-

---

77. 484 U.S. 518, 527 (1988).

78. *Id.* at 527 ("His [the President's] authority to classify and control access to information bearing on national security . . . flows primarily from this constitutional investment of power [U.S. Const., Art. II, § 2] in the President and exists quite apart from any explicit congressional grant.").

79. *See* Oglesby v. United States Department of the Army, 79 F.3d 1172 (D.C. Cir. 1996).

> As long as an agency declares through its affidavits that the responsive material has been reviewed to assure the continuing accuracy of its original classification, and that a determination has been made that the withheld information still poses a security risk if released, the mere passage of time is not a per se bar to reliance on exemption 1.

Id. at 1183.

80. Although the Bush Administration has not redefined the Government's classification scheme, President Bush has added the Secretary of Health and Human Services to the list of officials authorized to classify information. Exec. Order No. 12,958, 66 Fed. Reg. 64,347 (Dec. 10, 2001).

81. The "specifically authorized" language of Section 5 U.S.C. § 552(b)(1) has been narrowly construed by the courts. *See* Dep't of Air Force v. Rose, 425 U.S. 352, 361 (1976).

82. 610 F.2d 824 (D.C. Cir. 1979).

terests.[83] The court applied this precedent in *Afshar v. Department of State*,[84] holding that the burden of showing that information had been publicly disclosed falls on the plaintiff.[85] The posting of a web page to the Internet clearly qualifies as disclosure and publication. This argument has been tested in trade secret litigation, where the courts universally have accepted that web publication constitutes public disclosure.[86] Government information that has been posted on the Internet is thus no longer eligible for the national security exemption from the FOIA. Therefore, once information is posted to the Internet by the Federal Government, it must remain available to the public. Furthermore, under EFOIA, such information must remain available in electronic form.[87]

V. ANALYSIS

A. Information Can Be Dangerous

The American public requires information, but too much information can cause security problems. Unfortunately, the Internet poses a new problem: when it becomes necessary to clamp down on information, it may already be too late. The rapid transmission and copying of data on the Internet means that "[o]nce you put something on the Web, you have little control of where copies of it end up."[88] In general, with most publicly available information, this result is not problematic. If information is available for the public, then it should not matter whether the public can view the same information on one or one hundred websites.

However, when certain information on the Internet becomes useful to terrorists, there are problems. Even if the FOIA allowed for the removal of information from the public domain, the mass dissemination of information on the Internet prevents the contraction of information. In other words, it is faulty to assume "that information once available can later be restricted, that the toothpaste, in other words,

---

83. *Id.* at 831–32.

84. 702 F.2d 1125 (D.C. Cir. 1983).

85. *Id.* at 1130.

86. *See, e.g.*, Religious Technology Center v. Lerma, 908 F. Supp. 1362, 1368 (E.D.Va. 1995) ("[P]osting works to the Internet makes them 'generally known,' at least to the relevant people interested in the news group."); Religious Technology Center v. NetCom On-line Communication Services, Inc., 923 F. Supp. 1231, 1256 (N.D.Cal. 1995) ("Although the Internet is a new technology, it requires no great leap to conclude that because more than 25 million people could have accessed the newsgroup postings . . . these works would lose their status as secrets.").

87. *See* Part II(B), *supra*.

88. Dina Cappiello, *State Purges Web Sites*, THE TIMES UNION (Albany), Dec. 30, 2001, at A1 (quoting David Kennedy, director of research services at TruSecure Corp.).

can be put back in the tube, in the age of the Internet."[89] It is possible, then, that in its zeal to make Government information available online during the Clinton Administration, the Executive Branch posted too much information to the Internet prior to September 11. This does not imply that the Bush Administration should put an end to the era of Government disclosure on the Internet. Application of the FOIA principles discussed above and some common sense indicate that new measures are unnecessary.[90]

B. What Should Be Disclosed Now and in the Future?

Under the FOIA and because of the realities of the Information Age, information that the Government already has posted online is in the public domain, and it is too late to remove it. This does not mean, however, that such information must stay on the Internet without modification. Rather, the FOIA merely requires that these records remain available electronically for FOIA requests or in electronic reading rooms.[91] In fact, it may be perfectly appropriate to limit Internet access to some previously available Government information.[92] Electronic FOIA requests and even access to electronic reading rooms can be monitored, requiring at the very least the identity of the requesting or accessing individual. The return of this information to agency websites should thus be considered in the same manner as new information.

Unfortunately, there is no present standard for agency websites within the Executive Branch. Without direct guidance from Congress or the President since September 11, agencies have monitored their websites in an ad hoc manner.[93] For example, the Army has removed

---

89. *See* Robin Toner, *A Nation Challenged: Flow of Information*, N.Y. TIMES, Oct. 28, 2001, at 1B4.

90. *See* Beirle & Bell, *supra* note 42, at 9 ("Government agencies acted quickly in a crisis. But as the Russians say, 'nothing is so permanent as a temporary measure.' Hasty decisions may lock us into ill-conceived policies we may have to live with for a long time.").

91. The Department of Energy, for example, issued a policy statement on October 11, 2001, removing information from DOE websites and instructing interested parties to follow traditional FOIA request procedures. 66 F.R. 52917 (Oct. 18, 2001).

92. *See* Sabin Russell, *Web Sites Pull Information in Interest of National Security Fear of Giving Useful Data to Terrorists*, S.F. CHRON., Oct. 5, 2001, at A13 ("If there are people among us who are intent upon spectacular mass murders, then all of our security policies need to be recalibrated.") (quoting Steven Aftergood).

93. *See* Eckert, *supra* note 27, at A13 ("It may have been appropriate for agencies to limit public access in the immediate aftermath of the terrorist attacks. But . . . we have no public justification of those actions and we don't have any stakeholder involvement or criteria to determine when or whether information should be put back in the public domain.") (quoting Gary Bass, executive director of OMB Watch). The article also quotes Steven Aftergood, director of the Project on Government Secrecy at the Federation of American Scientists, as saying,

web pages from some divisions' websites, while leaving comparable information online for other divisions.[94] Access to many of the Army's web pages has also now been limited to persons seeking access from '.mil' servers.[95] As a result, many members of the active reserves no longer have access to needed information, while many non-military personnel, who simply access the Web through .mil servers, continue to have access.[96]

Through the FOIA and EFOIA, Congressional intent is clear: all non-classified Government information should be online. As the Executive Branch proceeds, Congress may need to step in to clarify the intent of the FOIA,[97] but the FOIA does not lack effect. As discussed earlier, the letter and spirit of EFOIA directs federal agencies to maintain informative websites. Agencies withholding information should be mindful that the national security exemption to the FOIA only applies to information specifically and properly classified under an Executive Order. Finally, under the interpretation of the FOIA that covers agency web pages as records, the Government must guarantee access to all information posted online, and the public need not worry that future threats will shut down the Internet.

VI. CASE STUDIES

The foregoing arguments are perhaps best considered through two brief case studies. This Part will discuss the DOT and the EPA. These two agencies have been selected for ease of discussion and as examples of how it may be proper or improper to remove or to limit access to web content.

A. The Department of Transportation's NPMS Website

Prior to September 11, the DOT maintained a detailed website for the National Pipeline Mapping System ("NPMS"). This website offered pipeline information to the general public, including detailed

> The problem we see is that so far most agencies are proceeding in an ad hoc manner without clear, defensible criteria for what they publish and what they remove .... We don't live in a monarchy and these decisions are not solely up to the president and the attorney general. Congress will have to step up and assert a larger public interest.

Id.

94. *See* Stephens, *supra* note 43 (stating "access criteria on previously public information is inconsistent and illogical").

95. *See id.*

96. *See id.*

97. *See* Toner, *supra* note 89 ("As agencies use the discretion they have on what information they put on line for the public, there also needs to be Congressional oversight to make sure that discretion is not abused.") (quoting a spokesman for Leahy).

maps and structural and safety information. Since September 11, however, the DOT has removed this information.[98]

The web page lists the Government officials and other professionals who may still gain access to necessary pipeline data through specific request and security-check procedures: "At this time, OPS is providing pipeline *data* (not access to the Internet mapping application) to pipeline operators and local, state, and Federal government officials *only*."[99] The general public no longer has any access to this information via FOIA request or otherwise.

The Department's offer of information to a limited segment of the requesting public (pipeline operators and Government officials) does not relieve the Department of its burden under the FOIA. Even if a requester has no urgent or even legitimate need for information, the FOIA requires Government disclosure. The FOIA explicitly states that Government records must be made "promptly available to any person."[100] This statutory language — "any person" — has been tested and upheld by the courts. In *United States Department of Justice v. Reporters Committee for Freedom of the Press*,[101] the Supreme Court held that "the identity of the requesting party has no bearing on the merits of his or her FOIA request."[102] Therefore, although it may have been legitimate for the DOT to remove pipeline information from the web, this information *must* remain public to *all* requesters. The requirements of the FOIA require that FOIA requests still be fulfilled, and if this information is subject to multiple FOIA requests, it must return at least to the Department's electronic reading room, where access can be monitored.

Looking into the future, the DOT must consider what information to withhold legitimately from the public. Traditionally, the information contained on the NPMS pages would not be exempt from the FOIA.[103] In the wake of September 11, however, Congress has followed up with a bill to give the Secretary of Transportation additional powers to withhold information.[104] Section 14, "Pipeline Security-

98. http://www.npms.rspa.dot.gov/data/npms_data_down.htm (last visited Jan. 22, 2002).

99. *Id.* (emphasis in original).

100. 5 U.S.C. § 552(a)(3).

101. 489 U.S. 749 (1989).

102. *Id.* at 771. *See also* Schwaner v. Dep't of Air Force, 898 F.2d 793, 798 (D.C. Cir. 1990) (acknowledging "the principle of disregarding the identity of the requester").

103. The closest exemption argument would be under exemption 9, which exempts "geological and geophysical information and data, including maps, concerning wells," 5 U.S.C. § 552(b)(9), but there is sparse additional information on exemption 9, and further discussion is unwarranted in these pages.

104. Pipeline Infrastructure Protection to Enhance Security and Safety Act, 2001 Cong. U.S. H.R. 3609 (Dec. 20, 2001).

Sensitive Information," of the proposed act amends 49 U.S.C.A. § 60117 with the following:

> If the Secretary determines that particular information obtained by the Secretary or an officer, employee, or agent in carrying out this chapter may reveal a systemic vulnerability of a pipeline system, or a vulnerability of pipeline facilities to attack, the information shall be withheld from public disclosure.[105]

This statutory language will provide the DOT the ability to withhold such information under exemption 3 to the FOIA, which exempts those records that are:

> 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.[106]

The proposed act would meet these criteria and would require the exemption of sensitive materials from FOIA disclosure. As stated, however, this exemption would only apply *prospectively* to agency information that has not already been disclosed and should only be considered for future actions by the DOT.[107] By following the guidance of the FOIA and with proper care for other existing statutes and Executive Orders regarding national security classification, the DOT need not view September 11 as an impetus for dramatic changes. The same can be said of the EPA.

B. The Environmental Protection Agency's Risk Management Plans

The EPA collects Risk Management Plans ("RMPs") from chemical companies under Section 112(r) of the Clean Air Act.[108] These plans provide vital information about dangerous chemicals being used in manufacturing plants, including hazard assessments, prevention programs, and emergency response plans. Prior to September

105. *Id.*

106. 5 U.S.C. § 552(b)(3).

107. The public disclosure limitation on exemption 1, discussed in *infra* Part IV, applies equally to claims for exemption 3. *See* Afshar v. Dep't of State, 702 F.2d 1125 (D.C. Cir. 1983).

108. 42 U.S.C. § 7412(r) (2001).

11, the EPA posted the RMPs to the agency's website with limited information excluded. RMPs contain sections that describe the worst case scenarios, called Offsite Consequence Analyses ("OCAs"). Although this information was barred from web publication by Congress after the FBI noted the temptation of OCA data to terrorists,[109] RMPs were posted to the Internet, and the OCA data remained available in designated reading rooms.

Since September 11, however, the EPA has identified and separately classified two types of RMP data files and posted the following statement to its website:

> (1) RMP files that do not contain OCA Information have been temporarily removed by EPA from its website in light of the September 11 [sic]. EPA is reviewing the information we make available over the Internet and assessing how best to make the information publicly available. We hope to complete this effort as soon as possible.
> (2) Files that contain OCA data are only available to "covered persons" . . . .[110]

The statement then proceeds to explain the nature of "covered persons" and provides a link to further information. The second of these limitations is acceptable,[111] but the first is unreasonable.

The dissemination of the EPA's RMP data files is hotly contested by community activists, political pundits, and chemical companies.[112] This issue has already been discussed and resolved by the FBI in the Executive Branch and Congress. By limiting access to OCA data, "[b]oth the FBI and Congress have acknowledged that disclosure through the Internet of the remainder of the RMP information pre-

---

109. *See* Gary Bass, *A Post-September 11 Attack on Right-to-Know*, OMB WATCH, Oct. 2, 2001, *at* http://www.ombwatch.org/info/2001/rtkstatement.html.

110. http://www.epa.gov/ceppo/review.htm (last visited Jan. 25, 2002).

111. The reclassification of information that has not been widely published is acceptable under the FOIA. In Afshar v. Dep't of State, 702 F.2d 1125 (D.C. Cir. 1983), the court held that changes in national security require, at times, such reclassification, and that the courts will not question the executive decision. It remains questionable, however, whether the OCA data withheld is now properly classified under the national security exemption to the FOIA.

112. *See* Knickerbocker, *supra* note 38, at 1 ("By restricting our right to know, even through a well-intentioned effort to protect safety, government is abandoning its duty to warn the public if a community is at risk.") (quoting Jeremiah Baumann, environmental health specialist at the US Public Interest Research Group). *But see* Jonathan H. Adler, *How the EPA Helps Terrorists*, NAT'L REV. ONLINE, Sept. 27, 2001, *at* http://www.nationalreview.com/comment/comment-adlerprint092701.html ("Once the government forces information about potential accidents to be disclosed, there is no controlling the use to which it could be put.").

sented no unique increased threats of terrorism. This is why EPA's decision to remove the entire RMP is quite startling."[113] Despite the EPA's understandable fears of further terrorist threats, the FOIA handles this situation very simply: because RMP data does not fall under one of the nine exemptions to FOIA disclosure, the EPA cannot withhold these records. Barring a new Executive Order or action by Congress to the contrary, the EPA should thus continue to provide full and open access of Risk Management Plans to the public.

VII. CONCLUSIONS

The events of September 11 have shaken our nation, and the Government is ready and eager to respond. Despite the American public's support of military action, however, a December 2001 *New York Times*/CBS poll indicates that the public "feels increasingly wary that the administration's effort will erode core civil liberties."[114] The Executive Branch, in its efforts to limit public access to potentially dangerous information, has ignored this sentiment and the requirements of the Freedom of Information Act, attempting to create new policy where old legal structures still apply. The most obvious of these changes is the removal of information from many Government websites.

Websites, like other agency materials, are "records" under the FOIA and thus deserve the same treatment as other agency records. The Internet does not require a new set of rules for Government disclosure but instead, until Congress acts, requires the application of traditional rules in a new context. Although little can be done about the Executive's reaction to the September 11 tragedy other than force the continued disclosure of once-public information by legal action if necessary, the Government should consider the FOIA's application to the Internet as it proceeds into the future. Where holes remain, Congress needs to step in, as it has done with the DOT, and give guidance regarding the Government's disclosure of information on the Internet.[115]

113. *See* Bass, *supra* note 109.

114. *See* Beirle & Bell, *supra* note 42, at 9.

115. *See* Cohen, *supra* note 57, at 30 ("Emergencies do not last forever, and as the sense of crisis ebbs, the other branches of government will no doubt step in again, as they have done throughout history.").