Title

Let The People Know the Facts: Can Government Information Removed From the Internet Be Reclaimed?

Publication Date

2006

Peer reviewed

Let the People Know the Facts: Can Government Information Removed from the Internet Be Reclaimed?*

Susan Nevelow Mart**

Ms. Mart examines the legal bases of the public's right to access government information, reviews the types of information that have recently been removed from the Internet, and analyzes the rationales given for the removals. She suggests that the concerted use of the Freedom of Information Act by public interest groups and their constituents is a possible method of returning the information to the Internet.

"Let the people know the facts, and the country will be safe."—Abraham Lincoln[1]

¶1 Popular information needed by "people who mean to be their own Governors"[2] has been disappearing from government agency Web sites on the Internet at an alarming pace, generally in the name of national security. However, much of the information removed has had little effect on national security, but its loss has had a deleterious effect on vitally important public issues, such as local environmental contamination,[3] women's health and employment parity,[4] and civil rights issues.[5]

¶2 Even where the information removed from the Internet might bear some relation to national security, such as the case of environmental data, recent analysis has shown that the information is not of the level of detail that would actually aid terrorists in planning a successful attack, so removing it has a disproportionately high

---

** Reference Librarian and Adjunct Professor of Law, University of California Hastings College of the Law Library, San Francisco, California.

1. *Quoted in* John Cornyn, *Ensuring the Consent of the Governed: America's Commitment to Freedom of Information and Openness in Government,* 17 LBJ J. PUB. AFF. 1, 8 (2004).
2. CITIZEN'S GUIDE TO THE FREEDOM OF INFORMATION ACT 1 (1987) (quoting letter from James Madison to W.T. Barry (Aug. 24, 1822), *in* IX THE WRITINGS OF JAMES MADISON 103 (G.P. Hunt ed., 1910)).
3. *See* Christopher H. Schmitt & Edward T. Pound, *Keeping Secrets: The Bush Administration Is Doing the Public's Business Out of the Public Eye. Here's How—and Why*, U.S. NEWS & WORLD REP., Dec. 22, 2003, at 18, *available at* http://www.usnews.com/usnews/news/articles/031222/22secrecy.htm.
4. *See* MARY THORN, NAT'L COUNCIL FOR RESEARCH ON WOMEN, MISSING: INFORMATION ABOUT WOMEN'S LIVES (2004), *available at* http://www.ncrw.org/misinfo/report.pdf. The report details, for example, the deletion of information on condom use from Web sites, *id*. at 8, and the removal of the *Handbook on Women Workers* and fact sheets on women workers from the U.S. Department of Labor site, *id*. at 12.
5. *See Democracy Now!: Civil Rights Commission Purges Reports Critical of Bush* (radio broadcast Feb. 16, 2005), *available at* http://www.democracynow.org/article.pl?sid=05/02/16/156238.

impact on citizens who need information.[6] As Nancy Kranich has eloquently stated, "[I]f the public's right to know is to be protected in today's world, citizens must have optimal opportunities to acquire and exchange information. The stakes are high, for as the Supreme Court noted years ago, American democracy requires 'the widest possible dissemination of information from diverse and antagonistic sources.'"[7]

¶3 This article discusses the bases of the public's right to government information and the types of such information that have been removed from federal government Web sites on the Internet. It considers whether the rationale given for such removals is appropriate. Finally, it suggests using the federal Freedom of Information Act (FOIA)[8] in an innovative manner to return the information to the Internet.

A Brief History of the Freedom of Information Act

¶4 The public's right to access government information is most visibly protected by FOIA, enacted in 1966 to stop an increasingly noticeable tendency by federal agencies to shroud their actions in secrecy.[9] Earlier attempts to solve the problem by piecemeal reform of the Administrative Procedure Act had not been successful in overcoming federal agencies' disinclination to release information.[10]

¶5 The Senate Committee on the Judiciary, charged with reporting on the bill introducing FOIA, reached the following conclusions: "A government by secrecy benefits no one. It injures the people it seeks to serve; it injures its own integrity and operation. It breeds mistrust, dampens the fervor of its citizens, and mocks their loyalty."[11]

---

6. John C. Baker et al., Rand Nat'l Defense Research Institute, Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information 71 (2004), *available at* http://www.rand.org/pubs/monographs/2004/RAND_MG142.pdf; *see also Emerging Threats: Overclassification and Pseudo-classification: Hearings Before the Subcomm. on National Security, Emerging Threats, and International Relations of the House Comm. on Government Reform*, 109th Cong. 121–26 (Mar. 2, 2005) [hereinafter *Emerging Threats Hearings*], *available at* http://reform.house.gov/UploadedFiles/Blanton%20Shays%20testimony%202%20March%202005.pdf (prepared statement by Thomas S. Blanton, Director, National Security Archive, George Washington University).
7. Nancy Kranich, The Information Commons: A Public Policy Report (2004), http://www.fepproject.org/policyreports/infocommons.contentsexsum.html (quoting Associated Press v. United States, 326 U.S. 1, 20 (1945)).
8. 5 U.S.C. § 552 (Supp. 2002).
9. Herbert N. Foerstel, Freedom of Information and the Right to Know: The Origin and Application of the Freedom of Information Act 10–28 (1999); *see also* S. Rep. No. 89-813, at 3 (1965) ("After it became apparent that section 3 of the Administrative Procedure Act was being used as an excuse for secrecy, proposals for change began.").
10. Foerstel, *supra* note 9, 39–40. After news media groups had worked for ten years to get a Freedom of Information Act passed, agencies were quick to find loopholes; in 1972, public interest groups, including Ralph Nader's, pushed for the 1974 FOIA amendments. Alan. B. Levenson & Harvey L. Pitt, Government Information: Freedom of Information Act, Sunshine Act, Privacy Act 1–2 (1978).
11. S. Rep. No. 89-813, at 10.

¶6 The debate about access to government information and the passage of FOIA took place at the same time that the Supreme Court was expanding its First Amendment jurisprudence. If FOIA had not been enacted, there might be a more explicit First Amendment protection of access to government information as a subset of the constitutionally protected right to receive information.[12] Although the right to know about all of the workings of the government may be implied in the right to petition the government,[13] the Supreme Court has limited access to government information as a matter of constitutional right to the press's right to information about certain trial proceedings.[14] Despite the Supreme Court's continued affirmation of a constitutionally protected right to *receive* information, the Court has relied on FOIA, not the Constitution, to protect *access* to other government information.[15]

¶7 As a statutory framework for protection of access to government information, FOIA defined the agency records that were subject to disclosure, set up a rebuttable presumption of mandatory disclosure, and granted nine exemptions.[16] Claiming an exemption is not mandatory; an agency has the discretion to release the information where no harm would result from the disclosure.[17] The Supreme Court has held that the nine "exemptions are specifically made exclusive . . . and must be narrowly construed."[18]

¶8 The FOIA was amended in 1974.[19] These amendments broadened the definition of agency, revised time limits for responding to FOIA requests, required agencies to make indexes of information more readily available, clarified congressional intent to allow *in camera* judicial review of allegedly classified documents in FOIA litigation, required annual reports to Congress, and granted courts discretion to award attorney's fees and court costs for successful litigants (who would be advancing "a strong congressional policy"[20]).[21] The amendments were not passed without a political battle. President Ford vetoed the amendments to FOIA, on the advice of Chief of Staff Donald Rumsfeld and Deputy Chief of Staff Richard Cheney that, among other concerns, the amendments would go too far in allowing judicial review of classified documents.[22] Antonin Scalia weighed in with arguments that the amendments were unconstitutional.[23] Congress overrode the veto.

---

12. FOERSTEL, *supra* note 9, at 66–67.
13. *Id*.
14. *See generally* Barry P. MacDonald, *The First Amendment and the Free Flow of* I*nformation: Towards a Realistic Right to Gather Information in the Information Age*, 65 OHIO ST. L.J. 249, 258–302 (2004).
15. From *Martin v. Struthers*, 319 U.S. 141 (1943), to *Reno v. ACLU*, 521 U.S. 844 (1997), the Supreme Court has recognized a constitutional right to receive information. *See generally* Susan Nevelow Mart, *The Right to Receive Information*, 95 LAW LIBR. J. 175, 2003 LAW LIBR. J. 11.
16. The exemptions are listed in 5 U.S.C. § 552(b) (2000).
17. Chrysler Corp. v. Brown, 441 U.S. 281, 293 (1979).
18. Dep't of the Air Force v. Rose, 425 U.S. 352, 361 (1976).
19. Pub. L. No. 93-502, 88 Stat. 1561 (1974).
20. H.R. REP. NO. 93-876, at 2, *reprinted* 1974 U.S.C.C.A.N 6267, 6267–68.
21. *Id*. at 6–7, *reprinted in* 1974 U.S.C.C.A.N. 6267, 6272.
22. Veto Battle 30 Years Ago Set Freedom of Information Norms (Dan Lopez et al. eds, National Security Archive Electronic Briefing Book No. 142, Nov. 23, 2004), http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB142.
23. *Id.*

¶9 Congress tinkered with FOIA for more than twenty years, tightening loopholes,[24] but the next major amendment was in 1996, when the Electronic Freedom of Information Act Amendments of 1996 (E-FOIA) was passed.[25] Two major provisions of E-FOIA require that:

> Each agency, in accordance with published rules, shall make available for public inspection and copying— . . . 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. . . .*[26]

> 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 or, if computer telecommunications means have not been established by the agency, by other electronic means.*[27]

¶10 Taken together, these two provisions require every agency to create "electronic reading rooms," and many agencies have in fact done so. The Department of Justice (DOJ) maintains an online list of more than a hundred department and agency electronic reading rooms.[28] Unfortunately, a 1999 study of agency compliance concluded that no agency had met the statutory deadlines for compliance with E-FOIA.[29] Agencies have not rushed to acquire the technical infrastructure necessary to comply with laws requiring Web posting of documents that agencies don't want to disseminate in the first place.[30]

¶11 The FOIA has been amended since 1996. In 2002, Congress added a blanket prohibition on intelligence agencies providing documents to foreign govern-

---

24. For example, the 1976 amendments, Pub. L. No. 94-409, § 5(b), 90 Stat. 1241, 1247, were Congress's attempt to strengthen judicial review of exemption 3 (exempting information governed by another statutory exemption), in response to a case deferring to the agency's broad interpretation of this exemption. *See* Michael H. Hughes, Note, *CIA v. Sims: Supreme Court Deference to Agency Interpretation of FOIA Exemption 3,* 35 CATH. U.L. REV. 279, 281 (1985). The 1986 amendment, Pub. L. No. 99-570, §§ 1802–03, 100 Stat. 3207, 3207-48 to -49, tried to clarify fees and fee waivers, as well as refine exclusionary language. FOERSTEL, *supra* note 9, at 55–56.
25. P.L. 104-231, 110 Stat. 3048 (1996).
26. § 4(5), 110 Stat. at 3049 (codified at 5 U.S.C. § 552(a)(2)(D) (2000) (emphasis added)).
27. § 4(7), 110 Stat. at 3049 (codified at 5 U.S.C. § 552(a)(2) (2000) (emphasis added)). Attempts to limit publication in electronic reading rooms on privacy grounds have not always been successful. *See, e.g.,* McCready v. Principi, 297 F. Supp. 2d 178, 198–99 (D.C. Cir. 2003) (holding that posting of final audit report, which included criticism of former Secretary, on the electronic reading room of the Veteran Administration's Web site did not violate the Privacy Act).
28. U.S. Dept. of Justice, Other Federal Agencies' FOIA Web Sites, http://www.usdoj.gov/04foia/other_age.htm (last visited Oct. 12, 2005).
29. Patrice McDermott, *An OMB Watch Update Report on the Implementation of the 1996 "E-FOIA" Amendments to the Freedom of Information Act*, GOV'T INFO. INSIDER, Spring-Summer 1999, *available at* http://www.ombwatch.org/info/efoia99/efoiareport.html. The report specifically found that of sixty-four agencies examined, 11% did not have a useful FOIA Web presence, 89% had varying compliance rates, and, as of November 24, 1999, no agency had complied fully with E-FOIA. McDermott found that the primary problems were lack of funding, lack of OMB guidance, lack of encouragement by DOJ to comply, and lack of agency emphasis on making public access to government information a priority.
30. *Id.* (citing Michael Tankersley, Introducing Old Duties to New Technologies 2 (1998)).

ments.[31] A much broader exemption was passed as part of the Homeland Security Act of 2002. Section 214 of the Act[32] exempts any information provided voluntarily by nonfederal entities or individuals that relates to infrastructure or other vulnerabilities to terrorism, which means that any business can protect information from a FOIA request merely by providing it to the Department of Homeland Security. This exemption is broad enough to overwhelm the balance FOIA has mandated between disclosure and secrecy.[33]

DOJ's Interpretation of FOIA Changes from Presumption of Disclosure to Promise to Defend

¶12 In every new administration, the attorney general sends out a memorandum discussing the Department of Justice's implementation of FOIA.[34] The Clinton administration enhanced FOIA's statutory presumption of disclosure. Even before the passage of the E-FOIA, Attorney General Janet Reno instructed all agency and department heads that documents should be provided to requestors unless the "agency reasonably foresees that disclosure would be harmful to an interest protected by" a particular exemption; she further indicated that doubts about whether or not a document fell within an exemption should be resolved in favor of disclosure.[35] Since FOIA was enacted to overcome the reluctance of agencies to reveal their workings to the public, the attorney general's memorandum sends a message, one way or the other, on how agency stubbornness in releasing documents will be viewed from above.

¶13 During the early days of the Bush administration, Attorney General John Ashcroft sent out his interpretation of FOIA's statutory presumption in favor of disclosure:

> 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*

31. P.L. 107-306, § 312, 116 Stat. 2383, 2390–91 (codified at 5 U.S.C. § 552 (a)(3)(E) (Supp. 2002)).
32. P.L. 107-296, § 214, 116 Stat. 2135, 2152–55 (2002) (codified at 6 U.S.C. § 133 (Supp. 2002)).
33. The Restoration of Freedom of Information Act of 2003, S. 609, 108th Cong. (2003), and a companion bill, H.R. 2526, 108th Cong. (2003), were introduced to narrow the exemption. Although the bills died in committee, the Senate bill has been reintroduced as the Restoration of Freedom of Information Act of 2005, S. 622, 109th Cong. (2005).
34. For a discussion of the role of the attorney general's memorandum in each new administration, see Kristen Elizabeth Uhl, Comment, *The Freedom of Information Act Post-9/11: Balancing the Public's Right to Know, Critical Infrastructure Protection, and Homeland Security*, 53 Am. U. L. Rev. 261, 269–70 (2003).
35. Memorandum from Janet Reno, Attorney General, to Heads of [All Federal] Departments and Agencies, The Freedom of Information Act (Oct. 4, 1993), *in* FOIA Update, 1999, no. 3, *available at* http://www.usdoj.gov/oip/foia_updates/Vol_XIV_3/page3.htm.

> *risk of adverse impact on the ability of other agencies to protect other important records*.[36]

¶14 Bush's Chief of Staff Andrew Card sent another memorandum further encouraging agencies to withhold documents in response to FOIA requests, asking agencies to withhold "any information that could be misused,"[37] an extremely broad category. In the additional guidance provided to agencies by a document attached to Card's memorandum (and prepared at his request), each agency was granted the discretion to determine what information should be "controlled" as "sensitive but unclassified," even if it did not otherwise meet the standards for classification or reclassification:

> *[D]epartments and agencies maintain and control sensitive information related to America's homeland security that might not meet one or more of the standards for classification set forth in Part 1 of Executive Order 12958. The need to protect such sensitive information from inappropriate disclosure should be carefully considered, on a case-by-case basis,* together with the benefits that result from the open and efficient exchange of scientific, technical, and like information.
>
> All departments and agencies should ensure that in taking necessary and appropriate actions to safeguard sensitive but unclassified information related to America's homeland security, they process any Freedom of Information Act request for records containing such information in accordance with the Attorney General's FOIA Memorandum of October 12, 2001, *by giving full and careful consideration to all applicable FOIA exemptions*.[38]

¶15 The proponents of open government on the House Committee on Government Reform were so angered by the Ashcroft memorandum that when they revised the *Citizens' Guide on Using the Freedom of Information Act*

---

36. Memorandum from John Ashcroft, Attorney General, to Heads of All Federal Departments and Agencies, The Freedom of Information Act (Oct. 12, 2001) (emphasis added), *available at* http://www.usdoj.gov/04foia/011012.htm.
37. Memorandum from Andrew H. Card, Jr., Assistant to the President and Chief of Staff, to the Heads of Executive Departments and Agencies, Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security (Mar. 19, 2002), *available at* http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm:

    > I asked the Acting Director of the Information Security Oversight Office and the Co-Directors of the Justice Department's Office of Information and Privacy to prepare guidance for reviewing Government information in your department or agency 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. Their guidance is attached, and it should be distributed to appropriate officials within your department or agency, together with this memorandum, to assist in your undertaking an immediate reexamination of current measures for identifying and safeguarding all such information at your department or agency.

38. Memorandum from Laura L.S. Kimberly, Acting Director, Information Security Oversight Office, Richard L. Huff & Daniel J. Metcalfe, Co-Directors, Office of Information and Privacy, Department of Justice, to Departments and Agencies (Mar. 19, 2002) (emphasis added), *available at* http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm#guidance. Some agencies have jumped on the "sensitive but unclassified" (SBU) bandwagon by creating multiple categories of pseudo-classifications that flag material that should be carefully considered before release, as the Centers for Disease Control did when it created twenty-seven new categories of SBU. Office of Sec. & Emergency Preparedness, Centers for Disease Control & Prevention, Sensitive But Unclassified Information (July 22, 2005), *available at* http://www.fas.org/sgp/othergov/cdc-sbu.pdf.

and the Privacy Act of 1974, which is edited and published from time to time by the committee, they included the following statement in the introduction: "Above all, the statute requires Federal agencies to provide the fullest disclosure of information to the public. . . . *Contrary to the instructions issued by the Department of Justice on October 12, 2001*, the standard should not be to allow the withholding of information whenever there is merely a 'sound legal basis' for doing so."[39]

¶16 Under these memoranda, agencies have been given the green light to deny FOIA requests, knowing that if there is any "sound legal basis" for doing so, the DOJ will defend them. Not surprisingly, 31% of FOIA officers responding to a 2003 GAO survey (57 of 183) said they were less likely to make discretionary disclosures of information; of these, 75% were primarily influenced by the Ashcroft memorandum.[40] Forty-eight percent of those responding to the GAO survey (88 of 193) noticed no change in making discretionary disclosure.[41] It is impossible to tell if those who did not notice a change in making discretionary disclosures previously had been enthusiastic or obstructive in complying with FOIA requests, but it is true that agencies have a long history of preferring to keep their information secret.[42]

¶17 While some agencies appear unaffected by the Ashcroft memorandum, it does make it more likely that a request will be denied. The only way to resolve a dispute over an agency's refusal to honor an FOIA request is through a lawsuit.[43] But the time and monetary cost of a suit means that access for most individuals is effectively denied, making public interest groups the default defenders of access to information. As a consequence, many lawsuits have been filed by public interest groups since October 2001, testing whether the courts will continue to virorously enforce FOIA.

¶18 There have been attempts in the 108th and the 109th Congresses to foreclose the attorney general's *regulatory* interpretation by enacting a *statutorily* mandated

---

39. A Citizens' Guide On Using the Freedom of Information Act and the Privacy Act of 1974 to Request Government Records, H.R. Rep. No. 109-226, at 3 (2005) (emphasis added).
40. U.S. Gen. Accounting Off., Freedom of Information Act: Agency Views on Changes Resulting From New Administration Policy 24 (GAO-03-981, 2003), *available at* http://www.gao.gov/new.items/d03981.pdf.
41. *Id*. at 14.
42. One form of agency obstruction is requesting excessive fees, despite a statutory mandate to charge only the reasonable costs of copying. 5 U.S.C. § 552(a)(3)(E)(4)(A)(ii)(II) (2000) (noncommercial requestors shall only be charged "reasonable standard charges for document duplication). For example, the DOJ requested advance payment of huge fees as a condition of responding to an FOIA request. Press Release, People for the American Way, Dept. of Justice Asks for Outrageous FOIA Fees in Secret Trials for 9-11 Detention Cases (Jan. 31, 2005), *available at* http://www.pfaw.org/pfaw/general/default.aspx?oid=17777. In April 2005, the DOJ dropped its $373,000 fee request. Dan Christensen, *Feds Drop $373,000 FOIA Search Fee Demand*, law.com, Mar. 4, 2005, http://www.law.com/jsp/article.jsp?id=1112349912757.
43. The 1974 amendments to FOIA expedited judicial review by setting a ten-day limit for the initial response and a twenty-day limit for a decision on the administrative appeal from a denial or failure to respond within ten days. 5 U.S.C. §§ 552 (a)(6)(A)(i)–(ii) (2000).

regulatory presumption in favor of disclosure. Representative Henry Waxman introduced the Restore Open Government Act of 2004 in the 108th Congress.[44] This bill seems at first glance to be unnecessary, in light of the statutorily mandated presumption of disclosure, but the bill is directed at removing the clout the DOJ's interpretation has on actual agency responses. This bill specified agency level responses to FOIA requests, repudiated the Ashcroft and Card memoranda, required a presumption in favor of disclosure, reinstated President Reagan's executive order on the release of presidential records, and reduced excessive classification.[45] Although the bill died in committee, it has been reintroduced in the 109th Congress.[46] Two other bills promoting FOIA reform introduced in the 109th Congress are the OPEN Government Act of 2005[47] and the Faster FOIA Act.[48] The OPEN Government Act would limit the ability to create new exemptions by implication; apply FOIA to outsourced record-keeping functions; protect access to FOIA fee waivers for legitimate journalists, regardless of institutional association (including bloggers and other Internet-based journalists); improve reporting requirements; require agencies to give people seeking documents a tracking number within ten days and to set up telephone or Internet systems allowing them to learn the status and estimated completion date; impose penalties for failure to comply, including the loss of all exemptions (except national security, personal privacy, proprietary information, or a ban in another law); and determine the appropriate funding levels needed to ensure agency FOIA compliance.[49] The Faster FOIA Act would establish a sixteen-member advisory Commission on Freedom of Information Act Processing Delays and would make recommendations to Congress and the president about reducing delays in processing FOIA requests.[50]

Removal of Information from Agency Web Sites

¶19 While the Bush administration is facilitating agencies' bureaucratic reluctance to provide information, access to information is also being blocked on another front.

¶20 After September 11, 2001, massive amounts of information began to disappear from government agency Web sites. In some instances, the terrorist attack was used as the explicit basis for the removal. In others, the information has just disappeared.[51]

---

44. H.R. 5073, 108th Cong. (2004).
45. Minority Staff, Comm. on Gov't Reform, U.S. House of Representatives, Summary: The Restore Open Government Act of 2004 (Sept. 14, 2004), http://democrats.reform.house.gov/features/secrecy_report/pdf/pdf_leg_restore_open_government_act_summary.pdf.
46. H.R. 2331, 109th Cong. (2005).
47. S. 394, 109th Cong. (2005); H.R. 876, 109th Cong. (2005).
48. S. 589, 109th Cong. (2005).
49. News Release, U.S. Senator John Cornyn, Cornyn, Leahy Introduce Bipartisan Bill To Promote Openness In Government (Feb. 16, 2005), *available at* http://cornyn.senate.gov/record.cfm?id=232212&ref=home.
50. News Release, U.S. Senator Patrick Leahy, Cornyn, Leahy Introduce Bill to Create Open Government Commission (Mar. 10, 2005), *available at* http://leahy.senate.gov/press/200503/031005.html.
51. OMB Watch, an agency oversight group, maintains a detailed register of missing information. OMB Watch, Access to Government Information Post September 11th, http://www.ombwatch.org/article/articleview/213/1/104 (last visited Oct. 26, 2005).

¶21 The Environmental Protection Agency's (EPA) removal of information from its Web site is a prime example of such action conducted ostensibly in the name of national security. After September 11, the EPA removed certain risk management plans (RMPs) from its site,[52] despite clear statutory directives that only the Offsite Consequence Analyses (OCA) portions of the RMPs were exempted from Internet posting.[53] RMPs contain information about chemicals being used in plants, including a hazard assessment, a prevention program, and an emergency response plan. In a recent round of rule making, the EPA acknowledged that Internet disclosure of RMPs that did not include the OCA information presented no unique increased threats of terrorism.[54] Nevertheless, RMPs are still missing from the EPA's Web site.[55] Environmental groups are calling for "mandatory security restrictions such as establishing anti-terrorist technology standards and a general duty clause for responsible, anti-terrorist chemical storage and handling" as a responsible substitute for the wholesale removal of information about the dangers to communities of certain chemicals.[56]

¶22 Another instance of "Web scrubbing" in the name of national security is the Federal Energy Regulatory Commission's (FERC) reconsideration of its Internet access polices in the wake of September 11th. The agency removed tens of thousands of documents regarding dams, pipelines, and other energy facilities.[57] The

52. The following notice was posted by the EPA (and last updated Oct. 22, 2001): "In light of the September 11 events, EPA has temporarily removed RMP Info from its website. 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 that effort as soon as possible." Chem. Emergency Preparedness & Prevention Office (CEPPO), U.S. Environmental Protection Agency, RMP Info—Temporarily Unavailable, http://www.epa.gov/OEM/rmp_unavailable.htm (last visited Oct. 26, 2005).
53. Paul M. Schoenhard, Note, *Disclosure of Government Information Online: A New Approach From an Existing Framework,* 15 HARV. J.L. & TECH. 497, 518–19 (2002). The OCA information had been removed from Internet distribution for an initial one-year period by legislation introduced in the 106th Congress. Chemical Safety Information, Site Security and Fuels Regulatory Relief Act, Pub. L. No. 106-40, 113 Stat. 207 (1999) (codified at 42 U.S.C. § 7412(r)(7)(H)(ii) (2000)). During that one-year period, OCAs were not subject to FOIA. § 7412(r)(7)(H)(iii).
54. Accidental Release Prevention Requirements, 69 F.R. 18819, 18824 (Apr. 9, 2004). The agency also agrees with the comment that removing OCA data from executive summaries would reduce or eliminate any risk that Internet posting of executive summaries might pose. The final regulations on posting this information on the Internet are at 40 C.F.R. § 1400.13 (2005). Under 42 U.S.C.§ 7412(r)(7)(H)(iii) (2000), these regulations supersede FOIA requests for the information covered by the regulations. However, the remainder of the information contained in the RMPs is not governed by these sections and are supposed to be available on the Internet. *See* OBM Watch, *supra* note 51, http://www.ombwatch.org/article/articleview/213/1/104/#EPA (risk management plans removed from EPA Web site).
55. The EPA has also limited access to its online Envirofacts databases; after registration, access is limited to EPA employees; EPA contractors; and military, federal, and state agency employees. *See* U.S. Environmental Protection Agency, Accessing the Envirofacts Database, http://www.epa.gov/enviro/html/technical.html#Accessing (last visited Oct. 26, 2005); OMB Watch, *supra* note 51, http://www.ombwatch.org/article/articleview/213/1/1/#EPA (no direct access to Envirofacts Databases).
56. Timothy R. Henderson, *September 11th: How It Has Changed a Community's Right to Know*, MD. B.J., July/Aug. 2002, at 3, 8.
57. OMB Watch, *supra* note 51, http://www.ombwatch.org/article/articleview/213/1/104/#FERC (FERC removes documents).

documents have not been replaced and public requests for information are now channeled to a special request page that requires registration (including the requestor's social security number) and agreement with limitations on the use and disclosure of any information provided.[58] The rationale for the removal may have a surface appeal, but a 2003 investigation strongly suggests that advancing the economic interests of favored industries or keeping executive actions from being scrutinized are the actual motivations.[59] The five-month investigation resulted in a long list of examples of information either removed from the Internet or prevented from ever getting there.[60] One fully documented instance involved FERC's refusal to give residents living near a proposed natural gas pipeline the list of the landowners potentially affected.[61] The information had previously been public, but FERC used terrorism as an excuse to deny a request for the information.[62] The landowners, of course, wanted to organize against the pipeline. The inability to get information affected their ability to mount effective opposition, and the pipeline was approved.[63]

¶23 Even more frustrating to advocates who need access to information about dangerous plants, removal of such information by the EPA and FERC has not improved security at affected plants. According to a Congressional Research analysis, in 2002 the *Pittsburgh Tribune-Review* investigated the security at potentially dangerous plants that were required to file RMPs and concluded that security was so bad that a reporter with a camera "could walk or drive right up to tanks, pipes, and control rooms considered key targets for terrorists."[64]

¶24 In a recent report prepared by the RAND Corporation, there is a detailed analysis of the EPA's Toxic Release Inventory (TRI) information from Envirofacts

58. Fed. Regulatory Energy Comm'n, How-to File a Critical Energy Infrastructure Information (CEII) Request, http://www.ferc.gov/help/how-to/file-ceii.asp (last visited Oct. 26, 2005).
59. Schmitt & Pound, *supra* note 3, at 18, 20, 22; *Now: Veil of Secrecy* (PBS television broadcast Dec. 12, 2003) (transcript available at http://www.pbs.org/now/transcript/transcript246_full.html). This was a joint investigation by *U.S. News and World Report* and the Public Broadcasting Service (PBS). Although the information provided by the published article and contemporaneous broadcast transcript frequently overlap, some is available in one source but not the other.
60. The article details missing energy information, tire and safety information, environmental information, transportation information, and the potential for misuse of critical infrastructure information laws to shield industry. Schmitt & Pound, *supra* note 3, at 22, 24–25, 27–28; *Now: Veil of Secrecy*, *supra* note 59.
61. *Now: Veil of Secrecy*, *supra* note 59 (remarks of interviewee Joseph McCormick).
62. *Id*.
63. *Id*.
64. Linda-Jo Schierow, Congressional Research Serv., Chemical Plant Security 12 (CRS Report No. RL31530, 2005) (quoting Carl Prine, *Lax Security Exposes Lethal Chemical Supplies*, Pittsburgh Tribune-Review, Apr. 7, 2002). Two of the plants the reporters visited were on the list of 123 plants nationwide where a worst-case scenario would affect more than 100,000 residents. "The report concluded that . . . access was easy to some sites owned by corporations with large security budgets; employees, customers, neighbors, and contractors 'not only let a stranger walk through warehouses, factories, tank houses and rail depots, but also gave directions to the most sensitive valves and control rooms'; and access to 19 sites was allowed due to 'unguarded rail lines and drainage ditches, dilapidated or nonexistent fences, open doors, poorly angled cameras and unmanned train gates.'" *Id.* (quoting Carl Prine, *Chemicals Pose Risk Nationwide*, Pittsburgh Tribune-Review, May 5, 2002). Walking around would give terrorists the detailed information needed to plan an attack that is not available in RMPs (which provide only the more general information needed to identify a site).

and the TRI Explorer, as it affected specific facilities.[65] The report first noted the public benefits of TRI data:

> First, it has helped communities better prepare for possible emergencies. Second, since industries are required by law to submit detailed tracking information, it has helped industries to understand and track hazardous chemicals at their facilities more effectively and to motivate them to reduce their use and emissions of such chemicals because of the public visibility of such information. Third, environmental and community watchdog groups have used this information to help put pressure on facilities to reduce their use and emissions of such chemicals and to improve local emergency preparedness. In fact, it is well known in the pollution prevention field that public TRI declarations have helped motivate many companies to implement more pollution prevention activities.[66]

The report then reviewed the many alternate sources for TRI information about a facility,[67] and concluded that because the TRI data has low usefulness, is widely available elsewhere, and is public domain information, it would be difficult and unnecessary to restrict access to the information.

> It would also diminish the public good that comes from providing local community access to information that can significantly affect the well-being of citizens. In addition, such restriction would not enhance security, since the information provided by TRI would still be easy to obtain from other sources.[68]

¶25 The RAND report balances the public good that comes from making information available with the risk of terrorists actually using the information. It concluded that the removed information had the benefits of assisting law enforcement, advancing knowledge, informing people about environmental risks, and helping communities prepare and respond to disaster.[69] Since most information identified in the report was simply not specific enough to actually facilitate an attack, the missing information did not uniquely benefit terrorists.[70] The RAND report concluded that there was no need to restrict public access to most geospatial information.[71] There is no need in the trade-off between security and openness to deny citizens access to such information. Much of the information the government is now trying to hide on the grounds of "national security" is accessible elsewhere, and the only people harmed by its disappearance are those with limited ability to access it. The RAND report examined 629 federal databases and concluded that "*fewer than 1 percent of federal data are both unique to federal*

---

65. BAKER ET AL., *supra* note 6, at 83.
66. *Id*.
67. *Id*. at 84 (noting that the information is also available from HUD's E-MAPS, the Department of Commerce's LANDVIEW, RTKNet from the Unison Institute, and Scorecard from Environmental Defense). State databases also contain some of this information. *Id*. at 85.
68. *Id*. at 87.
69. *Id*. at 100–03.
70. *Id. at* xxix. An example of information specific enough to be useful to a terrorist might be the location of a "choke point in a major power grid or telecommunications network." *Id.*
71. *Id.* at 125 ("Given the ready availability of alternative data sources, restricting public access to such geospatial information is unlikely to be a major impediment for attackers in gaining the needed information for identifying and locating their desired U.S. targets.").

sources and potentially useful to attackers' information needs, compared with about 6 percent that is potentially useful to the attacker and about 94 percent that our assessment found to have no usefulness or low usefulness."[72]

¶26 Recent testimony by Thomas S. Blanton, director of the National Security Archive, discussed the many dangers of secrecy. With only 10 to 20% of government documents properly classified and with new categories of pseudo-classified documents preventing access to even more information, the benefits of the broad dissemination of information are being overlooked.[73] Beneficial examples of open access include the captures of the Unabomber only after the FBI reluctantly agreed to give his crank letters to the *New York Times* and the Washington sniper only after a license plate number, kept secret by law enforcement, was leaked to the press. Additionally, the only instance cited by the 9/11 Commission that might have prevented the attacks was a statement by the terrorists' paymaster that had they known that Zacarias Moussaoui had been arrested at a flight school in Minnesota, bin Laden would have called off the attacks.[74] The 9/11 Commission concluded that only "publicity" could have "derailed the attacks."[75] Truly, publicity is the best disinfectant.[76]

¶27 Protecting the government from criticism is another reason that agency Web pages are removed. On April 8, 2005, the Defense Technical Information Center Joint Electronic Library took its entire library offline, apparently because several of the library's holdings, including the *Joint Doctrine for Detainee Operations*, were about to be criticized in the press.[77] Although most of the library was put back online the following week, the offending articles are still missing.

¶28 Other Web pages that have been removed from agency Web sites have no nexus at all with national security. The Web pages removed simply do not reflect the current administration's political agenda. Actions by the Department of Labor (DOL) exemplify this kind of agency Web scrubbing. According to a report issued

---

72. *Id. at* 69–70. This analysis means that the actions of the National Imagery and Mapping Agency in ending the online sale of large-scale maps to the public, OMB Watch, *supra* note 51, http://www.ombwatch.org/article/articleview/213/1/1#NIMA, cannot be justified on national security grounds. The scale of the maps does not give a terrorist the detailed information needed to carry out a planned attack, so removing the maps does nothing to prevent harm and keeps the American public from getting easy access to useful information.
73. *Emerging Threats Hearings*, *supra* note 6, at 124–25 (testimony of Thomas S. Blanton).
74. Nat'l Comm'n on Terrorist Attacks upon the U.S., The 9/11 Commission Report 247, 276, 541 n.107 (2004).
75. *Id*. at 276.
76. Paraphrasing Louis D. Brandeis, Other People's Money 92 (1914) ("Sunlight is the best disinfectant; electric light the best policeman.").
77. *Defense Doctrine Web Site Goes Dark*, Secrecy News, Apr. 8, 2005, http://www.fas.org/sgp/news/secrecy/2005/04/040805. *Secrecy News* reported the shutdown on April 8, 2005. The library was restored the following week, although the critical documents remain unavailable. *DOD Joint Electronic Library Back Online,* Secrecy News, Apr. 18, 2005, http://www.fas.org/sgp/news/secrecy/2005/04/041805. Some of the documents formerly accessible through the library are available from the Fed'n of Am. Scientists, Defense Department Intelligence and Security Doctrine, Directives and Instructions, http://www.fas.org/irp/doddir/dod/index.html (last visited Oct. 26, 2005), and Cryptome.org (www.cryptome.org).

by the National Council for Research on Women, the DOL removed information from its Web site that had long been available to help women negotiate workplace rights.[78] An ongoing series of fact sheets on women workers is no longer available, and a DOL publication, *Don't Work in the Dark—Know Your Rights,* also has been taken off the DOL's Women's Bureau page.[79]

¶29 The council's report also documents the removal of information on women's health from the National Cancer Institute Web site, specifically that concerning the absence of a link between abortion and breast cancer.[80] And information about condom use was removed from a Centers for Disease Control and Prevention Web site.[81]

¶30 Just after the 2004 election, the Civil Rights Commission removed twenty public reports from its Web site. The reports that were removed were critical of the Bush administration, including one called *Redefining Rights in America: The Civil Rights Record of the George W. Bush Administration*.[82] Seventeen of the reports are available on other Web sites.[83]

---

78. THORN, *supra* note 4, at 14 (providing chart of missing information on women's work, domestic violence, pay equity, and trafficking).
79. *Id. at* 12. A researcher's attempt to get a copy of the publication or other information on pay equity or worker's rights for women from the Women's Bureau extended to direct telephone contact, but the researcher was told "that no publications on workers' rights and fair pay per se were available at that time from the Bureau." *Id. at* 13. Another publication, the *Handbook on Women Workers,* has been removed and has never been re-released. *Id.* at 12.
80. The National Cancer Institute had had a report on its Web site informing women that there was no scientific basis for a suggested link between abortion and breast cancer. In 2002, that fact sheet was removed and replaced with a publication stating that studies showing the abortion/breast cancer correlation were inconsistent. *Id.* at 7. Only after a hundred experts gathered to hold a hearing on the issue was the National Cancer Institute forced to re-post the information that there was no increased risk of breast cancer associated with abortion. *Abortion and Breast Cancer,* N.Y. TIMES, Jan. 6, 2003, at 20.
81. Adam Clymer, *Critics Say Government Removed Sexual Material From Websites to Push Abstinence,* N.Y. TIMES, Nov. 26, 2002, at A18. Although the CDC said that the information was removed in 2001 to be updated, the Web site has not been updated and abstinence is being promoted instead.
82. *Democracy Now!: Civil Rights Commission Purges Reports Critical of Bush*, *supra* note 5.
83. *See, e.g.,* The Memory Hole, Reports Purged From the Website of the Civil Rights Commission, http://www.thememoryhole.org/usccr/purged.htm (last visited Oct. 27, 2005). The most critical report had been catalogued as a government document by the Government Printing Office. U.S. Comm'n on Civil Rights, Redefining Rights in America: The Civil Rights Record of the George W. Bush Administration, 2001–2004 (Sept. 2004), *available at* http://purl.access.gpo.gov/GPO/LPS54680. The use of PURLs (permanent uniform resource locators) for documents that have been cataloged as government documents has provided a means of access to some Web pages that have been removed by agencies. As the former superintendent of documents stated in 2002:

> A few agencies have removed electronic information products that we have cataloged and pointed to as part of the FDLP/Electronic Collection. We are redirecting the PURLs to agency notices or our own notice to explain the situation. A partner agency, the Department of Energy Office of Scientific and Technical Information, has pulled over 5,800 research reports from three national laboratories that were included in the Information Bridge. We have requested that these be reviewed and returned, as appropriate, for public access. Other agency withdrawals have been information beyond the purview of the FDLP.

Letter from Francis J. Buckley, Jr., Superintendent of Documents, to Depository Library Directors (Mar. 14, 2002), *available at* http://www.access.gpo.gov/su_docs/fdlp/withdraw.html.

¶31 One agency has invited public comment prior to removing information from the Internet. In November 2004, the National Geospatial-Intelligence Agency (NGA), which publishes international navigation and planning charts in English, announced its intention to withdraw the materials from its Web site in October 2005. According to announcement by the agency in November 2004, the action was intended to accomplish several objectives, including

> safeguarding the integrity of Department of Defense (DoD) aeronautical navigation data currently available on the public Internet; preventing unfettered access to air facility data by those intending harm to the United States, its interests or allies; upholding terms of bi-lateral geospatial data-sharing agreements; avoiding competition with commercial interests; and avoiding intellectual property/copyright disputes with foreign agencies that provide host-nation aeronautical data.[84]

The agency's decision to make national security a basis for removing the documents from the Internet is startling, given that the announcement came *after* the publication in April 2004 of a RAND report commissioned by NGA[85] which concluded that less than 1% of geospatial information available online posed a security risk.[86] Based on statements from John Baker, coauthor of the RAND report, Naomi Lubick wrote in *Geotimes* that "[i]t is better to keep data available in general . . . and restrict layers that may be more sensitive, protecting them with passwords or other measures to ensure that only the right people obtain access."[87]

¶32 The Overseas Basing Commission prepared a report that criticized Secretary of Defense Donald Rumsfeld's strategy for streamlining the military and posted the document on its Web site. After the Pentagon asserted that the report contained classified material, the commission removed the report from the site.[88] The commission claimed that the report was based only on public information and that the critical nature of the report was the real problem.[89]

---

84. Announcement of Intent to Initiate the Process to Remove Aeronautical Information From Public Sale and Distribution, 69 Fed. Reg. 67546 (Nov. 18, 2004).
85. BAKER ET AL., *supra* note 6.
86. "[W]e estimate that fewer than 1 percent of federal data are both unique to federal sources and potentially useful to attackers' information needs, compared with about 6 percent that is potentially useful to the attacker and about 94 percent that our assessment found to have no usefulness or low usefulness. *Given these results, we conclude that only a few of federal agency geospatial sources appear significant to attackers' needs*." BAKER ET AL., *supra* note 6, at 70. The same analysis would apply to the Nuclear Regulatory Commission's (NRC) action in completely shutting down its 700,000 document online reading room, then only restoring part of the library. *Nuclear Commission Restores Portions of Online Library*, OMB WATCHER, Nov. 15, 2004, http://www.ombwatch.org/article/articleview/2517/1/1. The offending documents were floor plans from several university nuclear labs. *NRC Removes All Information From Its Public Website*, OMB WATCHER, Nov. 2, 2004, http://www.ombwatch.org/article/articleview/2498/1/297. The NRC still maintains that the offending documents should not be available online, but scientists disagree; while the "information might aid terrorists a little . . . 'if someone is determined to do this, it won't help them much. If someone wanted to find this out, they can.'" *Id*. (quoting David Albright, Institute for Science and International Security).
87. Naomi Lubick, *Homeland Security and Geospatial Data*, GEOTIMES, July 2004, http://www.geotimes.org/july04/NN_homelandsec.html.
88. Mike Allen, *Basing Panel Criticizes Rumsfeld, Upsets Pentagon*, S.F. CHRON., May 16, 2005, at A5.
89. *Id.* Two of the critical reports were withheld from Congress, but *Secrecy News* obtained copies in August 2005. *Suppressed BRAC Critiques Disclosed,* SECRECY NEWS, Aug. 4, 2005, http://www.fas.org/sgp/news/secrecy/2005/08/080405.html.

¶33 The FBI asked the Senate Judiciary Committee to remove letters that had already been posted on its Web site, and the committee complied.[90] The letters had been posted after briefings on allegations made by Sibel Edmonds, previously a contract linguist for the FBI, who alleged that the FBI had "mishandled information that might have tipped the government to the Sept. 11 terrorist attacks before they occurred."[91] In May 2004, the Justice Department asserted that the information in the briefings and information resulting from the briefings was classified; the Judiciary Committee removed two of the letters from its Web site.[92] While Edmonds has been prevented from testifying before the 9/11 Commission on grounds of national security,[93] and her lawsuit for wrongful termination has been dismissed on the same basis,[94] the FBI has agreed that the letters cannot be retroactively classified and has entered into a judgment that the letters are properly the subject of an FOIA request.[95]

Recovering Electronic Content after Its Removal from Agency Sites

¶34 Since pages on agency Web sites are "records" under FOIA, even those that have been taken down are properly the subject of an FOIA request. FOIA "grant[s] a right to obtain and copy records held by government entities . . . including electronic formats."[96] In 1996, E-FOIA amended the definition of record to include electronic formats[97] and required agencies to make all records created after November 1, 1996, available by computer communications within one year after the record is created.[98] The DOJ interprets FOIA as requiring Web pages to be republished: "If you request records that already exist in an electronic format, the FOIA requires agencies in almost all cases to provide these records to you in that

90. The Memory Hole, Classified Letters Regarding FBI Whistleblower Sibel Edmonds, http://www.thememoryhole.org/spy/edmonds_letters.htm (last visited Oct. 27, 2005).
91. Chris Strohm, *Lawsuits Challenge Justice Department Efforts to Classify Previously Public Information*, DAILY BRIEFING, June 28, 2004, at http://www.govexec.com/dailyfed/0604/062804c1.htm.
92. The Memory Hole, *supra* note 90.
93. Democrats.com, FBI Whistleblower Breaks Ashcroft's Gag Order to Warn America that the 9/11 Report is a Massive Coverup (Aug. 4, 2004), http://archive.democrats.com/search.cfm?term=sibel%20edmonds.
94. Kevin Bohn, *FBI Translator Suit Dismissed Over Security Issues*, CNN, July 7, 2004, http://www.cnn.com/2004/LAW/07/06/fbi.translator.
95. Stipulation of Dismissal, Project on Gov't Oversight v. Ashcroft, Civ. No.1:04cv1032 (D.C. Cir. Mar. 9, 2004) (on file with author); *see also* Letter of Vesper Mei, U.S. Dept. of Justice, to Michael T. Kirkpatrick, Public Citizen Litigation Group (Feb. 18, 2005), *available at* http://pogo.org/m/gp/gp-02182005-JusticeDeptLetter.pdf (acknowledging that the letters are "releaseable in full, pursuant to the Freedom of Information Act").
96. Henry H. Perritt, Jr., *Sources of Rights to Access to Public Information,* 4 WM. & MARY BILL RTS. J. 179, 186 (1995).
97. 5 U.S.C. § 552(f)(2) (2000) ("'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").
98. § 552(a)(2).

same format, if that is what you prefer."[99] In its explanation of the changes E-FOIA made to the definition of agency records, the DOJ also defines agency records in a manner that includes Web pages:

> This definition appears to confirm existing general practices of treating information maintained in electronic forms as subject to the FOIA and, while it references no particular electronic item such as computer software, seems to broadly encompass information maintained in electronic form.[100]

¶35 Prior to the passage of E-FOIA, there were several cases limiting rights to computer access; the intent of the E-FOIA was to explicitly overrule those cases.[101] The House Report that accompanied the Act certainly defines records broadly enough to include Web pages, which existed in 1996, as well as future technologies.[102] There is a general test for whether or not the subject of an FOIA request is an agency record: "whether (1) the material has been created or obtained by the agency; and (2) the agency is in control of the material."[103]

¶36 It is hard to imagine a straight-faced denial that a Web page created and hosted by an agency is not an agency record, even though no case defining agency records in the FOIA context has expressly addressed a Web page posted on the Internet.[104] The language of the E-FOIA amendments and the legislative history make it clear that making new "electronic formats" available by putting them in "electronic reading rooms" by "electronic means" meant getting documents, whether originally created in paper or on the Web, and putting them on the Internet. That certainly is the interpretation of the DOJ: "The Electronic FOIA amendments embodied a strong statutory preference that electronic availability

---

99. U.S. Dep't of Justice & U.S. Gen. Services Admin., Your Right to Federal Records: Questions and Answers on the Freedom of Information Act and Privacy Act, http://www.pueblo.gsa.gov/cic_text/fed_prog/foia/foia.htm#format (last visited Oct. 29, 2005).
100. *Congress Enacts FOIA Amendments*, FOIA Update, 1996, no. 4, *available at* http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page1.htm.
101. *See* Henry H. Perritt, Jr., *Recent Development: Electronic Freedom of Information*, 50 Admin. L. Rev. 391, 395–97 (1998) (discussing rejection by H.R. Rep. No. 104-795 (1996), *reprinted in* 1996 U.S.C.C.A.N. 3448, 3462, of *Dismukes v. Dep't of the Interior*, 603 F. Supp. 760 (D.D.C. 1984) (holding that agency is not required to accommodate plaintiff's format preference under FOIA) and *SDC Dev. Corp. v. Mathews*, 542 F.2d 1116 (9th Cir. 1976) (holding that agency-created computer database was library material and not agency record in accordance with Records Disposal Act)).
102. *See* Schoenhard, *supra* note 53, at 509–11 (citing H.R. Rep. No. 104-795, at 6 (1996), *reprinted in* 1996 U.S.C.C.A.N. 3448, 3449).
103. *Id. at* 511 (citing Dep't of Justice v. Tax Analysts, 492 U.S. 136, 144–45 (1989)).
104. For purposes of the Federal Records Act, "'records' are defined as all books, papers, maps, photographs, machine readable [i.e., electronic] materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business 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. . . .'" Armstrong v. Executive Office of the President, 1 F.3d 1274, 1278 (D.C. Cir. 1993) (citing 44 U.S.C. § 3301 (2000)). The Federal Records Act definition of records has been utilized in FOIA actions. *See, e.g.*, Weisberg v. U.S. Dep't of Justice, 631 F.2d 824, 828 (1980) (court looked to the provisions of the Federal Records Act in defining the phrase "agency records" in FOIA).

be provided by agencies in the form of online, Internet access—which is most efficient for both agencies and the public alike. . . .”[105] Once on the Internet as Web pages, documents do not lose their status as agency records. The impetus of E-FOIA has been to extend disclosure requirements to all records, regardless of their format, and Web pages should be no different.[106]

¶37 Once information has been posted on the Internet, it has entered the FOIA form of the “public domain.”[107] Web pages are by their nature widely published, and an FOIA request for a Web page that has been taken down is in reality just a request to have the same information in the same format republished. Mere publication of classified information does not automatically put the information in the public domain, but if the information is “well publicized,” then “suppression . . . would frustrate the aims of the FOIA without advancing countervailing interests.”[108] Web publication has been accepted, albeit reluctantly, by the DOJ as so “well publicized” that the documents posted on the Internet cannot be recalled.[109] Consequently, such material cannot be reclassified.[110] The “well publicized” rule is set forth in *Afshar v. Department of State*: the person requesting agency records under FOIA is required to “bear the initial burden of pointing to specific information in the public domain that appears to duplicate that being withheld.”[111] In the case of Web pages removed from the Internet, the person requesting agency records will be able to carry

105. Office of Info. and Privacy, U.S. Dep’t of Justice, Freedom of Information Act Guide (2004) (footnotes omitted), http://www.usdoj.gov/oip/readingroom.htm.

106. *See, e.g.*, Yeager v. Drug Enforcement Admin., 678 F.2d 315, 321 (D.C. Cir. 1982) (holding that method of accessing information can’t be used to circumvent full disclosure policies of FOIA).

107. Cottone v. Reno, 193 F.3d 550, 554 (D.C. Cir. 1999) (citations omitted) (In discussing the public domain doctrine, the court noted that “materials normally immunized from disclosure under FOIA lose their protective cloak once disclosed and preserved in a permanent public record. For as we have recently observed, ‘the logic of FOIA’ mandates that where information requested ‘is truly public, then enforcement of an exemption cannot fulfill its purposes.’”); Davis v. U.S. Dep’t of Justice, 968 F.2d 1276, 1279 (D.C. Cir. 1992) (“We have held, however, that the government cannot rely on an otherwise valid exemption claim to justify withholding information that has been ‘officially acknowledged’ or is in the ‘public domain.’”); *see also* Schoenhard, *supra* note 53, at 512–14; Edward Lee, *The Public’s Domain: The Evolution of Legal Restraints on the Government’s Power To Control Public Access Through Secrecy Or Intellectual Property,* 55 Hastings L.J. 91, 123 (2003) (“[I]nformation falls into the public domain when it becomes available to the public (without IP protection).”).

108. Schoenhard, *supra* note 53, at 513–14 (citing Founding Church of Scientology v. NSA, 610 F.2d 824, 831–32 (D.C. Cir. 1979).

109. Stipulation of Dismissal, *supra* note 95; *see also* Letter of Vesper Mei, *supra* note 95; Schoenhard, *supra* note 53, at 14 (citations omitted) (“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. Government information that has been posted on the Internet is thus no longer eligible for the national security exemption from the FOIA.”).

110. Exec. Order No. 13292, § 1.7(c)(2), 68 Fed. Reg. 15,315, 15,318 (Mar. 28, 2003) allows the reclassification of previously declassified material only if “the information may be reasonably recovered.” Once information is on the Internet, and available in whole or in part on other Web sites, it can’t reasonably be “recovered.” The FBI finally conceded that you can’t unring the bell.

111. 702 F.2d 1125, 1130 (D.C. Cir. 1983) (citations omitted).

this burden. The information will be identical in every way. The disclosure will be specific and will exactly match; a requestor will only be asking for an exact duplicate of what was previously available.

¶38 While nothing in FOIA prevents removal of information from agency Web sites, FOIA does require that information previously published be made available, in an electronic format. If the Web page was previously well publicized on the Internet, none of the FOIA exemptions will apply. There are other statutes directing agencies to post information on the Web, such as portions of the Paperwork Reduction Act of 1995[112] and the E-Government Act of 2002.[113] Once the information has been posted on the Internet, permanent public access is the statutory goal.[114] Although Web pages differ from written records in the ease with which they can be removed from public access, they are still government documents and, as such, are records that form a part of the history of the country. The Federal Records Act prohibits the destruction of government records, except in accordance with statutorily mandated procedures.[115]

¶39 Despite these statutory mandates for transparency in government and the retention and preservation of agency materials, a recent report commissioned by Representative Henry A. Waxman (D. Calif.) found that the Bush administration has "radically reduced the public right to know,"[116] and that its policies "are

112. 44 U.S.C. §§ 3506(4)(C), 3506(4)(G), 3511 (2000); *see also* 36 C.F.R. § 1234.1 (2005) ("establish[ing] basic requirements related to creation, maintenance, use, and disposition of electronic documents").

113. 44 U.S.C. §§ 3601–3606 (Supp. 2002). The government has been somewhat slow to understand the need to index, archive, and preserve electronic documents, but a plan has been put in place with the E-Government Act. Lee, *supra* note 107, at 168–69 (citations omitted) (discussing the Act's requirements that every federal agency "'establish a process for determining which Government information the agency intends to make available and accessible to the public on the Internet and by other means,'" that a "'federal Internet portal that will integrate agency Web sites'" be created, and that a "'public domain directory of public Federal Government Web sites'" be established). Lee thought the "efforts to build an online space for the public domain offer perhaps the greatest step forward for attaining the public domain's full promise: the public's free access to vast amounts of sources of learning." *Id.* at 169 (footnote omitted); *see also* Memo from Joshua B. Bolten, Director, Office of Management and Budget, to All Department and Agency Heads, Implementation Guidance for the E-Government Act of 2002 (Aug. 1, 2003) (establishing a timetable for record keeping for government Internet documents), *available at* http://www.whitehouse.gov/omb/memoranda/m03-18.pdf.

114. 44 U.S.C. §§ 207, 3501 nt, 3602(e)(5) (Supp. 2002).

115. 44 U.S.C. §§ 3301–3303a, 3308–3311 (2000). *See* U.S. Dep't of Educ., Federal Records Act, http://www.ed.gov/policy/gen/leg/fra.html (last visited Oct. 30, 2005) (providing excellent overview of the Act's requirements); HAROLD C. RELYEA, CONGRESSIONAL RESEARCH SERV., ELECTRONIC GOVERNMENT: A CONCEPTUAL OVERVIEW 26 (CRS Report No. RL30745, 2001), *available at* http://www.ipmall.piercelaw.edu/hosted_resources/crs/RL30745_Sept_10_2001.pdf (listing some of the information that has become freely accessible on the Internet as result of electronic government initiatives, but noting that two important matters remain to be addressed: the length of time documents or data are available on the Web and the subsequent retrieval from online archives, and the ability to make online FOIA requests for records and information not otherwise available online).

116. MINORITY STAFF, COMM. ON GOV'T REFORM, U.S. HOUSE OF REPRESENTATIVES, SECRECY IN THE BUSH ADMINISTRATION 4 (2004) (quoting fax from Philip H. Melanson, Professor of Policy Studies and Director, Policy Studies Program, Univ. of Massachusetts at Dartmouth, to House Government Reform Committee minority staff, The Bush Administration and FOIA (July 10, 2004)), *available at* http://democrats.reform.house.gov/features/secrecy_report/pdf/pdf_secrecy_report.pdf.

not only sucking the spirit out of the FOIA, but shriveling its very heart."[117] The report also concludes that "[n]o president in modern times has done more to conceal the workings of government from the people."[118]

¶40 E-FOIA may provide some cumbersome relief from this climate of secrecy. If agency Web pages removed from the Internet are considered agency *records*, then E-FOIA requires agencies to make electronic copies available 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 [FOIA] requests. . . ."[119] If concerned groups make multiple FOIA requests for removed Web pages, the agency is obligated to make those documents available in its electronic reading room. There is no overall standard for determining how many requests will trigger the reading room requirement.[120] However, many agencies have published regulations about repeatedly requested records.[121] The majority of them leave the determination of how many requests it takes, or whether or not records are likely to be repeatedly requested, entirely to the agency (subject to the absolute requirement that such documents must be posted online). Those agencies that do specify a number to limit agency discretion specify between three

117. *Id*. at 30 (quoting e-mail from Barbara Croll Fought, Associate Professor, S.I. Newhouse School of Public Communications, Syracuse University, to House Government Reform Committee minority staff (July 16, 2004)).

118. *Id*. at 31 (quoting e-mail from David C. Vladeck, Associate Professor, Georgetown Univ. Law Center, to House Government Reform Committee minority staff (June 22, 2004)). The top-level trend toward more secrecy is having a trickle-down effect on agency action; the FBI, for example, is trying to limit the scope of the searches it must perform in response to an FOIA request. In one case, the FBI performed an automated search that failed to find any documents responding to a request, even though searches through other channels showed that relevant documents had been released in response to a previous FOIA request. The indexes the FBI searched are not complete. Michael J. Sniffen, *FBI Tries to Limit Info Searches*, CBS NEWS, Jan. 21, 2005, http://www.cbsnews.com/stories/2005/01/21/national/main668365.shtml.

119. 5 U.S.C § 552(a)(2)(D) (2000) (emphasis added).

120. The Office of Management and Budget's failure to provide guidance to agencies by establishing a "clear definition of what constitutes a repeatedly requested record" is one of the criticisms made about FOIA implementation in a report published by OMB Watch. McDermott, *supra* note 29. The report notes that it is not "up to the *agency* to decide if it is interested in disseminating the information; it depends solely on whether outsiders submit multiple requests for this information. . . . [I]nformation that is of sufficient interest to the public to spark two or more request[s] must be placed in the agency's reading room and, if created since November 1, 1996, must be made available electronically and in such a way that anyone with online access will enjoy the same informational access." *Id.*

121. Three general types of regulations have been promulgated. Some regulations list the factors guiding agency discretion in determining whether or not a document has been requested often enough to be posted in an electronic reading room. *See, e.g.*, 7 C.F.R. § 1.4(a)(4) (2005) (Department of Agriculture); 32 C.F.R. § 701.14 (d) (2005) (Department of the Navy). Most agencies leave it entirely up to the agency. *See, e.g.*, 37 C.F.R. § 102.2 (c)(2) (2005) (United States Patent and Trademark Office); 15 C.F.R. § 4.2(d)(2) (2005) (Secretary of Commerce). Finally, some agencies actually specify the number of requests that will require posting in an electronic reading room. *See, e.g.*, 36 C.F.R. § 1250.12 (a)(4) (2005) (National Archives and Records Administration); 32 C.F.R. § 806.12 (2005) (Department of the Air Force); 26 C.F.R § 601.702 (b)(1)(D) (2005) (Internal Revenue Service).

and five requests.[122] Since the electronic reading room requirements were intended to avoid duplicative efforts and increase access to useful materials,[123] the small number is not surprising.

¶41 Public interest groups interested in recovering removed Web pages could create and publicize places on their Web sites where individuals could make concerted requests for the Web pages by posting something like the FOI Letter Generator.[124] An additional radio button could give users the option to send a copy of their request to the host of the Web site, so that any eventual administrative appeal or lawsuit seeking to have an item permanently posted to the agency's reading room could state with assurance the number of requests that had been made. The rule is that if enough people ask, the material must be posted to an electronic reading room. And the number of people does not have to be large. Three requests could be sufficient.

¶42 The use of Web sites and letter generators to make a significant impact on federal policy is not new. A recent example is the concerted efforts of the Parents Television Council and the American Family Association Commission, who have bombarded the Federal Communications Commission (FCC) with copies of the same Internet-generated letters. Almost 100% of the indecency complaints the FCC received in 2003 and 2004 were from these two groups.[125] There are sufficient numbers of people interested, both personally and through various nonprofit groups, in each of the categories of Web pages that have been removed from the Internet to make multiple FOIA requests a reasonable possibility. Then, of course, the requestors will have to deal with the aftermath: the potential refusal of the requests, administrative appeal, and filing suit.[126]

---

122. NARA requires posting if there have been three requests, 36 C.F.R. § 1250.12 (a)(4); the Air Force requires posting if there have been or are likely to be five or more requests, 32 C.F.R. § 806.12(b); and the IRS requires posting if there have been more than four requests, 26 C.F.R § 601.702 (b)(1)(D)(2).

123. H.R. Rep. No. 104-795, at 11 (1996), *reprinted in* 1996 U.S.C.C.A.N. 3448, 3454 ("[T]he information technology currently being used by executive departments and agencies should be used in promoting greater efficiency in responding to FOIA requests. This objective includes using technology to let requestors obtain information in the form most useful to them. Existing technologies for searching electronic records can often review materials more quickly than is possible via a paper review.").

124. Reporters' Comm. for Freedom of the Press, FOI Letter Generator, http://www.rcfp.org/foi_letter/generate.php (last visited Oct. 31, 2005) ("This letter generator is designed to help you create a simple FOI letter. It asks you for all pertinent information, guides you through the options available, and even lists a number of federal agencies and their addresses."). A similar form could be created by any public interest group seeking to have interested parties make multiple FOIA requests.

125. Melanie McFarland, *TV 2004: Janet Jackson's, uh, Expose Really Set Off The Sensors Of The Censors,* Seattle Post, Dec. 30, 2004, at C1. The statistics exclude the Super Bowl incident involving Janet Jackson. McFarland reports on the alleged 159 complaints from the Parents Television Council about *Married by America* that led to a $1.2 million fine. An investigation revealed that, in fact, there were only ninety complaints about the show, made by twenty-three individuals (with twenty of those copies of a letter written by a single person). The Parents Television Council responded that its members sent in 4073 complaints about the show.

126. Administrative appeal is normally a prerequisite to suit. Spannaus v. U.S. Dep't of Justice, 824 F.2d 52, 57–58 (D.C. Cir. 1987) ("It goes without saying that exhaustion of remedies is required in FOIA cases."); *see also* U.S. Dep't of Justice, Freedom of Information Act Reference Guide (Apr. 2005), http://www.usdoj.gov/04foia/referenceguidemay99.htm#appeals.

Court Action to Compel Disclosure under FOIA

¶43 An agency climate of nondisclosure will result in more lawsuits being filed to compel disclosure. The agency response to an FOIA request that Web pages removed from the Internet be provided in the same format may not be immediately favorable. Multiple FOIA requests for the same Web pages may not have a higher chance of success. Only pages that have actually been produced in response to an FOIA request would be required to be posted to an agency's electronic reading room,[127] but to avoid a second lawsuit over *where* the Web pages should be posted, any lawsuit to enforce compliance with multiple FOIA requests for the same pages (when the multiple requestors all want them produced as Web pages[128]) should include a request to the court to specify where the pages should be posted. The district court should have discretion, under the Declaratory Judgment Act, to declare where the requested Web pages should be posted.[129] Since E-FOIA requires the pages to be posted in the agency's electronic reading room, a request to do so would not be unreasonable.

¶44 Many agencies have been slow to follow the requirement that records that have been or will become the subject of repeated requests be posted in electronic reading rooms.[130] While courts are still deferring to agency characterizations of

---

127. 5 U.S.C. § 552(a)(2)(D) (2000). One commentator has suggested that FOIA may require agencies to take the initiative and post documents that they know will be of wide public interest in electronic readings rooms without waiting for requests. Michael Tankersley, *Introducing Old Duties to New Technologies*, FED. LAW., Sept. 1998, at 24, 27.

128. FOIA gives the district courts explicit statutory authority to review agency decisions to withhold records *de novo*. 5 U.S.C. § 552 (a)(4)(B) (2000). The requestor has the discretion to specify the format of the records being requested. 5 U.S.C. § 552 (a)(3)(B) (2000) ("In making any record available to a person under this paragraph, an agency shall provide the record in any form or format requested by the person if the record is readily reproducible by the agency in that form or format.").

129. 28 U.S.C. § 2201 (2000). An agency does not have discretion about posting frequently requested documents in an electronic reading room, so its discretion to determine the number of requests that trigger the obligation cannot be absolute. The legislative history establishes a mandate to post materials on the Internet to avoid multiple FOIA requests and the concomitant duplication of agency resources. *See supra* ¶ 40. This policy has been implemented in an OMB circular directing agencies, when providing information to the public, including under the Freedom of Information Act, to disseminate information in a way that "achieves the best balance between the goals of maximizing the usefulness of the information and minimizing the cost to the government and the public." Office of Mgmt. & Budget, Circular No. A-130, Management of Federal Information Resources § 8(a)(5)(d)(i) (Nov. 28, 2000), *available at* http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf.

130. *See* McDermott, *supra* note 29 (finding that no agency reading room contains all of the statutorily mandated material, and that "fewer than 30% of the sites examined contained FOIA-released repeatedly requested documents"). Elsewhere, McDermott pointed out that the requirement that agencies put up information that has been released on an FOIA request—and for which they anticipate more requests—is "way more honored in the breach than the observance. Agencies mostly put up trivia if they put up anything." Posting of Patrice McDermott, Assistant Director, American Library Association, Office of Government Relations, to GOVDOC-L@LISTS.PSU.EDU (May 25, 2005, 10:19:35) (copy on file with author).

documents as exempt for a variety of security-based reasons,[131] the burden is still on the agency to prove that there is an exemption.[132] For example, in *Gordon v. Federal Bureau of Investigation*, Judge Charles R. Breyer found that the government had not met its burden of proving an exemption to the plaintiffs' claims for information about the "no-fly" list. The court held:

> "The Supreme Court has interpreted disclosure provisions broadly, noting that *the act was animated by a 'philosophy of full agency disclosure.*'" Nonetheless, FOIA contains nine exemptions which a government agency may invoke to protect certain documents from public disclosure. "Unlike the disclosure provisions of FOIA, *its statutory exemptions 'must be narrowly construed*.'"
>
> The agencies resisting public disclosure—here, the FBI and TSA—have "the burden of proving the applicability of an exception." "That burden remains with the agency when it seeks to justify the redaction of identifying information in a particular document as well as when it seeks to withhold an entire document."[133]

Judge Breyer found that the agencies had labeled information that was innocuous as sensitive and had "offered no justification for withholding such information."[134]

¶45 The Bush administration's interpretation of FOIA dispenses with the presumption of access and essentially gives agencies carte blanche to deny access. Since the number of FOIA requests has increased dramatically,[135] admin-

---

131. James T. O'Reilly, *FOIA and Fighting Terror: The Elusive Nexus Between Public Access and Terrorist Attack,* 64 La. L. Rev. 809, 821–22 (2004) (estimating that agencies have won summary judgment motions in about 90% of litigated cases, by offering agency affidavits on the nature of the documents being withheld). *But see* Office of Info. & Privacy, U.S. Dep't of Justice, New FOIA Decisions October–December 2004, FOIA Post, Jan. 10, 2005, http://www.usdoj.gov/oip/foiapost/2005foiapost1.htm (of twenty-eight cases reported, only five appear to have been resolved by agency declaration as to the nature of the documents being withheld); Office of Info. & Privacy, U.S. Dep't of Justice, New FOIA Decisions January–March 2005, FOIA Post, Mar. 31, 2005, http://www.usdoj.gov/oip/foiapost/2005foiapost9.htm (of fifty-nine cases reported, twenty-one appear to have been resolved by agency declaration as to the nature of the documents being withheld). This mini-survey of FOIA lawsuits does not confirm a 90% claim.

132. Athough only classified documents are explicitly exempt from FOIA disclosure pursuant to 5 U.S.C. § 552(b)(1) (2000) (exempting those documents that are "(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) are in fact properly classified pursuant to such Executive order"), several recent cases have shielded "pseudo-classified" documents labeled "sensitive, but unclassified" or "for your eyes only" under a number of theories. *See Emerging Threats Hearings*, *supra* note 6, at 8, *available at* http://reform.house.gov/UploadedFiles/Hammitt%20Testimony.pdf (prepared statement of Harry Hammitt, Editor/Publisher, *Access Reports*) (citing Living Rivers, Inc. v. Bureau of Reclamation, No. 2:02-CV-644TC (D. Utah, Mar. 25, 2003) (accepting agency's declaration that law enforcement maps of flood areas below the Hoover and Glen Canyon dams might aid terrorists in carrying out an attack); Coastal Delivery Corp. v. Customs Service, No. 02-3838 WMB (C.D. Cal., Mar. 14, 2003) (upholding use of exemption 2 protecting internal documents as basis for denying information regarding inspections of seaport operations because if terrorists knew how often inspections occurred, they could send their containers to vulnerable ports)).

133. No. C 03-01779 CRB, 2004 WL 1368858 (N.D. Cal.) (June 15, 2004) (citations omitted) (emphasis added).

134. *Id.*

135. OpenTheGovernment.org, Secrecy Report Card: Qualitative Indicators of Secrecy in the Federal Government 8 (Aug. 6, 2004), http://www.openthegovernment.org/otg/secrecy_reportcard.pdf (noting that from 2000 to 2003, FOIA requests have increased dramatically, from 2,174,570 to 3,266,394).

istrative appeals and lawsuits have become the norm. Nonetheless, only one of these lawsuits has been directed at information that has been removed from the Internet. The *Project on Government Oversight v. Ashcroft* suit[136] involved the DOJ's efforts to classify letters from Senate Judiciary Committee members to the FBI and the Justice Department regarding Sibel Edmonds; the letters had been posted on the Senate Judiciary Committee Web site but removed when the DOJ asserted that information in the letters was classified.[137] The complaint alleged that the letters could not be classified once posted on the Internet,[138] and the suit was settled by the government's agreement that the documents were subject to an FOIA request and the assurance that the plaintiffs would not be subject to any liability for posting the documents on the Internet.[139] The suit fell short of an enforceable order requiring an agency to post documents in an electronic reading room. But the clear language of E-FOIA compels such a conclusion.

The Balancing Act

¶46 The problem of enemy access to unclassified but possibly dangerous information is not a new one. During World War II, a German spy named Edmund Heine gave a German car manufacturer reports about the American aviation industry. The information was "lawfully accessible" from ordinary publicly available sources, including books, magazines, technical journals, trade fairs, and newspapers. The spy's conviction for failing to register as an foreign agent was upheld, but the espionage conviction was overturned. Commentator Edward Lee quotes the Second Circuit's conclusion, "'Certainly it cannot be unlawful to spread such information within the United States,'"[140] and then goes on to note that "[a]lthough the Second Circuit's decision did not explicitly use the term 'public domain,' subsequent courts and commentators have done so in explaining this limitation on espionage law."[141]

¶47 According to Lee, the court in Heine was "[s]olicitous of 'the spread of information' that was lawfully available to the public,"[142] that is, in the public domain. Once in the public domain, it is protected by the First Amendment.

---

136. Complaint for Declaratory and Injunctive Relief at 1, Project on Gov't Oversight v. Ashcroft, Civ. No.1:04cv1032 (D.C. Cir. June 23, 2004), *available at* http://www.citizen.org/documents/ACF681C.pdf.
137. *See supra* ¶ 33 for discussion.
138. Complaint for Declaratory and Injunctive Relief, *supra* note 136, at 1, 6.
139. Stipulation of Dismissal, *supra* note 95; *see also,* Letter of Vesper Mei, *supra* note 95 ("The FBI has acknowledged that these documents are releaseable in full, pursuant to the Freedom of Information Act.").
140. Lee, *supra* note 107, at 131 (quoting United States v. Heine, 151 F.2d 813, 815 (2d Cir. 1945)) (citations omitted).
141. *Id*. (citations omitted).
142. *Id*. at 132.

> [T]here is a danger that the government may prevent members of the public from using information already in the public domain, whether it be information related to national security, information revealed in open court or related to criminal or governmental proceedings, information subject to classification, or information sought under FOIA. But, in each of these areas, the public domain acts as a restraint against the government's attempts to restrict the flow or use of information already available to the public. The cases recognize that, while the government has an interest in maintaining secrecy, the interest is generally outweighed by the public's interest in the spread of the information once it is already available to the public. Paralleling the Copyright Clause's bar against removing material from the public domain through the grant of IP, the First Amendment prohibits the government from removing material from the public domain through secrecy.[143]

¶48 E-FOIA was a statutorily mandated expansion of the public domain. E-FOIA requires agencies to create an online location "where the public can obtain immediate access to government records."[144] If Web pages are removed, E-FOIA gives the requestor the right to require that the information be provided as a Web page. When more than two requestors seek access to the information through a FOIA request, the Web pages are required to be posted to the reading rooms.

¶49 Agencies have been and continue to be unprepared to deal with the requirements of E-FOIA.[145] The DOJ has acknowledged that there has been incomplete compliance with the requirements of E-FOIA, particularly the mandate to make certain categories of information available to the public electronically, including "records that are 'frequently requested' by FOIA requesters, which must be made available in their FOIA-processed form."[146] Information removed from the Internet had already entered the public domain by virtue of its prior publication on the Internet and is therefore "releasable under FOIA."[147] Even conservative think tanks like the RAND Corporation have concluded that the government has been overzealous in removing information from the Internet that citizens need to access. Open access to information has had an unlikely supporter in the person of Donald Rumsfeld who, in 1966, said in support of the passage of FOIA: "[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."[148]

---

143. *Id*. at 137–38.
144. Michael Tankersley, *How the Electronic Freedom of Information Act Amendments of 1996 Update Public Access For the Information Age*, 50 ADMIN. L. REV. 421, 428 (1998).
145. *Id*. at 429.
146. Memorandum from Richard L. Huff & Daniel J. Metcalfe, Co-Directors, Office of Information and Privacy, U.S. Dep't of Justice, to Principal FOIA Administrative and Legal Contacts at All Federal Agencies, Further Efforts to Implement E-FOIA Provisions (Mar. 23, 2001), http://www.usdoj.gov/oip/2001gaomemo.htm.
147. Stipulation of Dismissal, *supra* note 95.
148. Mark Tapscott, Too Many Secrets, WASH. POST, Nov. 20, 2002, at A25 (quoting Donald Rumsfeld, June 20, 1966, "advocating passage of the FOIA, of which he was a co-sponsor").

¶50 Groups interested in disclosure must band together to challenge the removal of documents from the Internet and the current administration's shifting of the burden of producing documents. This can be accomplished by making concerted FOIA requests for the missing Web pages and engaging in such administrative and judicial follow-up as is necessary. Organizations such as the American Federation of Scientists, Project on Open Government, National Security Archive, and individual scholars and citizens have uncovered massive amounts of information the government might have wished to keep secret.[149] But secrecy in government should be the exception, not the norm; that is what the Freedom of Information Act was intended to accomplish. FOIA has been enacted, amended, and repeatedly tinkered with over the years to accomplish openness in government. But it has always needed the actions of concerned citizens to keep it vital.

149. For discussion of just a few notable FOIA lawsuits, see Project on Gov't Secrecy, Fed'n of Am. Scientists, Freedom of Information Act Documents, http://www.fas.org/sgp/foia/index.html (last visited Nov. 1, 2005); Elec. Privacy Info. Ctr., Litigation Docket, http://www.epic.org/privacy/litigation (last visited Nov. 1, 2005); Public Citizen Litigation Group & Freedom of Info. Clearinghouse, Obtaining Access To Government Records Since 1972: Highlights Of Advocacy Efforts Against Government Secrecy (Jan. 1998), http://www.citizen.org/litigation/free_info/foic_aids/articles.cfm?ID=758.