2009

The Internet's Public Domain: Access to Government Information on the Internet

Susan Nevelow Mart
University of Colorado Law School

The Internet's Public Domain: Access to Government Information on the Internet

By Susan Nevelow Mart

Information on the Internet has an ephemeral character. It's easy to put up, and it's easy to take down. The ease with which online reality can change has concerned historians, librarians, archivists, and Internet visionaries like the founder of the Internet Archive[1] since the early days of the worldwide Web. When the source of the information is the government, the ephemeral nature of online information is even less acceptable. Congress has concurred in this sentiment. Although Web pages differ from written records in the ease with which they can be removed from public view, 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.[2] So information that has been removed should not have been destroyed, and once published on the Internet, information has entered the public domain.[3]

Information disappears from government Web sites in a number of ways. Sometime it is just changed in the normal course of business, and older versions of the Web site, although they should be archived by the government, generally are not.[4] Sometimes the removal has security overtones, as has been the case with information removed from government agency Web sites after 9/11 in the name of national security. Sometimes the reason for removal is to prevent political embarrassment or because information does not comport with the prevailing government policy, as has happened with some information on civil rights, environmental contamination, women's health and employment issues, and global warming.

Even when the reason for removing information has been national security, too much information may be removed. In the case of geospatial data removed after 9/11, for example, analysis has shown that a large percentage of 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 impact on citizens who need information.[5] Critical energy infrastructure information is another example where excessive removal of information is impairing citizen access to information critical to informed decision making on serious environmental issues.[6]

There is, of course, no dispute that certain information should be protected in the name of national security. But too much of what has been classified should not have been. The government's own experts estimate that between 50 percent and 90 percent of information that has been classified is improperly classified.[7] So if too much information has been removed from the Internet, either in the name of national security or for some reason of political expediency, how can the information be recovered? This article discusses some major examples of information that have been removed from federal government Web sites and suggests some innovative uses of the Freedom of Information Act (FOIA)[8] for returning the information to the Internet.

REMOVAL OF INFORMATION FROM AGENCY WEB SITES

After September 11, massive amounts of information began to disappear from government agency Web sites. In some instances, the terrorist attacks were used as the explicit basis for the removal. In others, the information just disappeared, and motives must be deduced from the context of the removal.[9]

THE ENVIRONMENTAL PROTECTION AGENCY

The Environmental Protection Agency's (EPA's) removal of information from its Web site is a prime example of removal conducted ostensibly in the name of

Susan Nevelow Mart received her JD from Boalt Hall School of Law and her MLIS from San José State University. Before becoming a librarian, she practiced law for nearly 20 years, focusing on real estate and business litigation. She is now the Faculty Services Librarian and an Adjunct Professor of Law at UC Hastings College of the Law and teaches advanced legal research there. She has written and presented extensively on the right to receive information, FOIA, the Patriot Act, and other legal issues affecting access to information. Susan Nevelow Mart, 2008. *This article is based and expands on "Let the People Know the Facts: Can Government Information Removed from the Internet Be Reclaimed?," 98* Law Libr. J. *1 (2006), available at* http://www.aallnet.org/products/pub_llj_v98n01/2006-01.pdf.

national security. After September 11, the EPA removed certain risk management plans (RMPs) from its site,[10] despite clear statutory directives that only the Offsite Consequence Analyses (OCA) portions of the RMPs were exempt from Internet posting.[11] 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 rulemaking, the EPA acknowledged that Internet disclosure of RMPs that did not include OCA information presented no unique increased threats of terrorism.[12] The information was approved for release, but still remains offline, and industry likes it that way.[13]

The EPA has also limited access to information on its Envirofacts database, the database that the EPA created in part to fulfill its statutory mandate to make Toxic Release Information (TRI) available electronically.[14] Only government employees and contractors who register online can get access to the full database.[15] Also, the EPA has limited reporting requirements for TRI information, so less data is available for inclusion in the TRI databases.[16] Since May 2002, the EPA Administrator has had the right to classify *any* information as secret that the Administrator determines might be a security risk.[17]

TRI information is the kind of information needed by residents to make sure that the environment that they live in is kept as clean as possible. A RAND Report that performed a detailed risk assessment for online geospatial information found that, for potential attackers, TRI data was not of significant use and that limiting access to this data had a disproportionately high impact on the health and welfare of the American public and a disproportionately low impact on terrorism prevention.[18] Yet public access to the data is still limited.

National security data restriction is not the only bar to public access to information at the EPA. In a recent report, the Union of Concerned Scientists reported on the political pressure that the Bush administration had been putting on EPA scientists.[19] From 2002 to 2006, political pressure silenced the EPA climate change Web site.[20] Although the revamped Web site now includes accurate scientific information, a close look reveals continuing political interference.[21] For example, the Web site does not reference important government reports such as the "National Assessment of Climate Change Impacts" and the "U.S. Climate Action Report."[22] The revised Web site has a "State of Knowledge" page that over-emphasizes uncertainty in climate change science.[23] The Union of Concerned Scientists' report also surveyed scientists at the EPA regarding the types of interference that they had experienced, and 24 percent responded that they had personally experienced frequent or occasional "disappearance or unusual delay in the release of websites, press releases, reports, or other science-based materials."[24]

The effort to suppress global warming science at the EPA continues. In *Massachusetts v. EPA*, the Supreme Court required the EPA to promulgate rules regulating greenhouse gases, but news reports revealed that the White House suppressed the EPA's response because the document completely refuted administration claims that applying the Clean Air Act to global warming would have "crippling effects on our entire economy."[25] The suppressed report estimates a net benefit to the economy of from one half to two trillion dollars.[26]

THE FEDERAL ENERGY REGULATORY COMMISSION

Another instance of Web scrubbing in the name of national security is the Federal Energy Regulatory Commission's (FERC's) reconsideration of its Internet access polices in the wake of September 11. The agency removed tens of thousands of documents regarding dams, pipelines, and other energy facilities.[27] All "information concerning proposed or existing critical infrastructure (physical or virtual)" has been designated "critical energy infrastructure information" (CEII).[28] The documents have not been replaced, and public requests for information are now channeled to a special request page that requires registration and agreement to limitations on the use and disclosure of any information provided.[29] A CEII requester has to agree, *inter alia*, to talk about CEII only with another recipient of the identical CEII, not to let anyone see the documents except other recipients of the identical material, and to be bound to secrecy unless the agency or a court finds that the information does not qualify as CEII; there are criminal and civil sanctions for violation.[30]

Although the most recent rules now allow landowners access to alignment sheets for the routes across or in the vicinity of their properties,[31] the information can't be shared or publicized, blocking use for advocacy, for notification of impending or future dangers, or for community awareness. This has had an impact on communities across the United States. Although protecting CEII sounds like a good idea, once again too much information is being protected, and several recent investigations strongly suggest that advancing the economic interests of favored industries or keeping executive actions from being scrutinized are the actual motivations.[32]

One such investigation resulted in a long list of examples of information either removed from the Internet or prevented from ever getting there, including the removal of tire and safety information, missing energy information, environmental information, and transportation

information, as well as the misuse of critical infrastructure information laws to shield industry.[33] For example, FERC refused to give residents living near a proposed natural gas pipeline the list of the landowners potentially affected.[34] The information had previously been public, but FERC used terrorism as an excuse to deny a request for the information.[35] The landowners, of course, wanted to organize against the pipeline, but their failure to get information affected their ability to mount an effective opposition, and the pipeline was approved.[36]

In 2004, the Center for Public Integrity filed a FOIA suit against FERC, alleging that FERC had improperly withheld documents relating to proposed liquefied natural gas (LNG) plants all over the country.[37] One particular instance involved a Fall River, MA, plant, where local residents were concerned about their community's safety and security, but correspondence between the builder and FERC were labeled CEII, effectively barring the pubic from finding out what was being planned.[38] The Center for Public Integrity believes that FERC "is aggressively undermining the authority of state and local governments to reject dozens of proposed liquefied natural gas facilities all across the country."[39] These residents certainly feel that politically motivated policy decisions may be hiding behind the veil of national security.

The FERC CEII non-disclosure agreement that requesters must sign appears on its face to be a gag order that acts as a prior restraint on speech and may violate First Amendment rights in much the same way that the broad reach of national security letter gag orders were found to violate the First Amendment.[40] A challenge to the current FERC regime by a CEII requestor on First Amendment grounds might be one way to improve access to any improperly classified materials in the FERC database.

THE DEPARTMENT OF TRANSPORTATION

Before September 11, the Department of Transportation (DOT) maintained a detailed Web site for the National Pipeline Mapping System (NPMS). This Web site offered pipeline information to the general public, including detailed maps and structural and safety information. Since 9/11, however, the DOT has removed this information.[41] Now, the public can get access only to regional level maps, whose level of detail is not useful if one wants information about a home, community, or neighborhood.[42] The Web page lists who may still access pipeline data: "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."[43] A post-September 11 bill would have given the Secretary of Transportation the authority to exempt from FOIA any of this information that the Secretary determined might reveal a vulnerability, but that portion of the bill didn't pass.[44] So there is no categorical exemption that the DOT could use in responding to a FOIA request for the information in an online format.

THE ARMY'S REIMER DIGITAL LIBRARY AND THE MARINE CORPS' DOCTRINAL LIBRARY

In February 2008, blogs and listservs lit up with the information that the Army was taking down its Reimer Digital Library, which is the largest online collection of US Army doctrinal publications. The Army had moved the collection behind a password-protected firewall, stating that: "It was a policy decision to put it behind a firewall and to restrict public access."[45] The move came as a surprise since only unclassified and non-sensitive records had ever been made available at the library site, a fact that the Army acknowledged.[46] Putting the documents behind a firewall not only restricted public access but also prevented other military branches from accessing the information. The Federation of American Scientists (FAS) made a FOIA request for the entire online library, and in response, the Army appears to have put the doctrinal library back online.[47]

The Marine Corps removed its online collection of unclassified doctrinal publications in March 2008.[48] FAS filed another FOIA request, asking for copies of all the documents so that they could be hosted on the FAS Web site. Again, the response was generally positive; although the official Marine Corps doctrine site is password-protected, the unclassified documents that were removed have been reposted at the main Marine Corps Web site.[49]

SMALL BUSINESS ADMINISTRATION

Another example where political expediency may be the rationale for removing information is the case of the Small Business Association's (SBA's) Central Contract Registry (CCR) Web site. In 2006, the SBA began removing data on the revenue of small companies from this Web site in the midst of an investigation that revealed that many of the businesses given government contracts under the program were not eligible.[50] The *Miami Herald* had published a report in 2005 documenting impropriety in SBA awards, and a television news team was compiling data from the CCR Web site when information on the size of businesses disappeared and was replaced with the following notice: "A firm's actual revenues and number of employees are not releasable under the Freedom of Information Act."[51] So only the SBA is in a position

to monitor compliance. But in 2006, the House Small Business Committee released *Scorecard VII*,[52] documenting billions of dollars in small business set-aside contracts that had been awarded to big businesses. Facilitating continuing public oversight of SBA contract awards seems like a necessary policy.

To try and get the information, the American Small Business League filed a FOIA request for the names of all the recipients of federal small business contracts and the contract amounts for 2005 and 2006. In the lawsuit that followed the SBA's refusal to provide the information, the SBA asserted that it had no list of the recipients or the contract amounts, since it gave raw data to the General Services Administration (GSA), providing GSA with parameters that GSA then uses to extract information from the database.[53] The district court found that argument implausible and said that "application of codes or some form of programming to retrieve" information found in computer records "constitutes a 'search' for existing records" and that "requesting the SBA to direct GSA to generate computer code to extract and compile the list of small businesses and contract amounts requested by the League is encompassed in the SBA's obligation to 'search' for electronic records."[54] The SBA has appealed the court's ruling.[55]

JOHNS HOPKINS POPLINE DATABASE

In April 2008, a medical librarian doing a search for abortion research on POPLINE, self-described as the world's largest database on reproductive health and run by Johns Hopkins' Bloomberg School, did not get same the results as in previous searches.[56] When she called, the librarian discovered the word "abortion" had been designated a "stop" word, or an unsearchable term, since late February.[57] This was confirmed by Johns Hopkins, which had completely deleted the word's searchability as a result of a complaint by USAID about the inclusion of one magazine's articles in the database.[58] The outcry was immediate and spread to the national newspapers; Johns Hopkins had to publicly explain and change its policy.

SIBEL EDMONDS

In 2004, the FBI asked the Senate Judiciary Committee to remove letters from its Web site that discussed allegations made by Sibel Edmonds, previously a contract linguist for the FBI, that the FBI had "mishandled information that might have tipped the government to the September 11 terrorist attacks before they occurred."[59] The Justice Department asserted that the information in the briefings and information resulting from the briefings was classified, despite the fact that the information had been given to Congress in 2002 and the letters had been posted on the Internet.[60] The Committee removed the letters. A lawsuit was filed regarding the attempted reclassification, and as part of a stipulated dismissal, the FBI agreed in principle that the letters could not be retroactively classified.[61]

THE BALANCING ACT: NATIONAL SECURITY VERSUS THE SOCIETAL BENEFITS OF ONLINE PUBLIC ACCESS

If information is removed in the name of security, one question is: Has the removal been effective? In the case of the EPA and FERC, advocates who need access to information about dangerous plants have been frustrated that removal of such information by the EPA and FERC has not improved security at affected plants.[62] According to the Congressional Research Service reports, 2002 and 2004 investigations of security at potentially dangerous plants that were required to file RMPs 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.[63]

Another question that information removal raises is: Does the information need to be kept secret because it is especially helpful to terrorists? In the RAND Report, the analysts balanced the public good that comes from making information available with the risk of terrorists actually using the information and 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.[64] 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.[65] The RAND report concluded that there was no need to restrict public access to most geospatial information.[66]

There is no need in the trade-off between security and openness to deny citizens access to such information. Much of the information that the government is now trying to remove from the Internet on the grounds of national security is accessible elsewhere; 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 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."[67]

So not very much in the way of geospatial information needs to be removed from the Internet to keep America safe. And a large percentage of every kind of document that the government classifies should be unclassified. As Thomas Blanton testified at the Emerging Threats hearings:

> From 50 percent, said the Pentagon's Deputy Under Secretary of Defense for Counter-Intelligence and Security, beyond 50 percent is what Mr. Leonard said. Sixty percent is what the Interagency Security Classification Appeals has done, ruled for the requestor. Seventy-five percent is what Tom Kean, the chair of the 9/11 Commission said. Ninety percent was the estimate of President Reagan's own National Security Council Executive Secretary in quotes to the Moynihan Commission. That's how much overclassification, 50 to 90 percent. Bottom line, you can sum it up, Houston, we have a problem.[68]

While the balance would appear to be in favor of less classification and more online public access, reversing current trends is extremely difficult. While some information is in fact properly classified, despite the widespread evidence of the amount of improper classification, the courts have been extremely deferential to agency classification characterizations.[69] And the Bush administration's climate favored agency secrecy.[70] It remains to be seen whether the policy changes made by the Obama administration can reverse the trend.[71] While FOIA is a fairly blunt tool for promoting public access, it is the tool that is available.

FOIA, E-FOIA, AND ADVOCACY

An increased climate of secrecy has fostered increased attempts to access government information. The number of FOIA requests has increased about 760 percent, from slightly less than 2.5 million in 2002 to more than 21.5 million in 2007.[72] Funding has not kept pace, increasing slightly less than 18 percent over this same period.[73] To enforce requests, requestors are still filing administrative appeals and lawsuits. So far, only one lawsuit has been directed at information that has been removed from the Internet. The *Project on Government Oversight v. Ashcroft* suit involved the Sibel Edmonds letters.[74] The complaint alleged that the letters could not be classified once posted on the Internet, and the suit was settled by the government's agreement that the documents were properly the subject of a FOIA request and the assurance that the plaintiffs would not be subject to any liability for posting the documents on the Internet. Because of the stipulated judgment, the suit did not result in a citable holding that documents once posted on the Internet cannot be reclassified, but the DOJ's stipulation is consistent with existing law on the nature of information once it is in the public domain.

For example, in trade secret litigation, courts have accepted that publication on the Internet is public disclosure.[75] And public domain information cannot form the basis for an espionage conviction. 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.[76] Previously classified information is *available*, or in the public domain, if it is "widely publicized."[77] Posting information on the Internet is a fair assurance that information is widely publicized.

There is a difference of course in how items might enter the public domain in intellectual property law and in government secrecy law, but for both, the public domain marks a line where protection ceases: Documents in the public domain cannot be kept from public access and use either on the grounds of intellectual property protection or on the grounds of secrecy:

> Courts have long recognized the concept of the public domain as a restraint on the government's power . . . these cases show that: (1) information falls into the public domain when it becomes available to the public (without IP protection); and (2) the First Amendment protects the public's ability to access and further disseminate information already in the public domain.[78]

Since the most current Executive Order allows reclassification only on condition that, *inter alia*, the information "may be reasonably recovered,"[79] information on the Internet cannot meet the legal requirements for re-classifying documents. Once information has been posted on the Internet, it has entered the FOIA form of the public domain.Web pages are by their nature widely published, and a 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."[80]

The Electronic Freedom of Information Act (E-FOIA)[81] 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," and the definition of records was expanded to include electronic formats.[82] If Web pages are removed, E-FOIA gives the requestor the right to require that the information be provided as a Web page, and 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.[83]

Since pages on agency Web sites are "records" under FOIA, even those that have been taken down are properly the subject of a FOIA request. 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.The language of the E-FOIA amendments and its 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 be provided by agencies in the form of online, Internet access—which is most efficient for both agencies and the public alike. . . ."[84] 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.[85]

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. 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.[86]

MULTIPLE FOIA REQUESTS

The climate of secrecy in the Bush administration was unparalleled. A 2004 House Report found that the Bush administration has "radically reduced the public right to know"and concluded that "[n]o president in modern times has done more to conceal the workings of government from the people."[87] 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 . . . 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. . . ."[88]

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.[89] There is no overall standard for determining how many requests will trigger the reading room requirement. However, many agencies have published regulations about repeatedly requested records.[90] The majority of them leave the determination of how many requests it takes, or whether 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 and five requests, and since the electronic reading room requirements were intended to avoid duplicative efforts and increase access to useful materials,[91] the small number is not surprising.

Public interest groups seeking to recover 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.[92] 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.

The use of Web sites and letter generators to make a significant impact on federal policy is not new. 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.

SINGLE FOIA REQUESTS FOR HOSTING ON THE REQUESTOR'S SERVER

At least one public interest group has been using the FOIA successfully to restore documents to the Internet.

The two FOIA requests filed by FAS requested a "softcopy of all unclassified, publicly releasable contents" of the digital libraries that had been removed from the Internet for hosting on the FAS server.[93] This request bypassed the electronic reading room as a hosting site completely. Although the documents were republished online on the agencies Web sites as a result of the FOIA requests, a comment on the FAS blog underscored the problem of agency Web hosting:

> The lesson here is that no one should assume that any document made available by a federal agency will continue to be available in the future. Any document—no matter what its status is with respect to public availability—can disappear at any time. We should have learned that lesson after 9/11. Anyone with an interest in agency document online [*sic*] should make and maintain a copy some where that the agency cannot reach. The only exception that occurs to me would be for documents required to be made public by law. If the RDL is put back online, FAS should nevertheless make a copy and keep it on its own servers in the future.[94]

These two FOIA requests were an effective use of targeted requests to change agency posting policy. Part of the reason that the strategy worked may have been the fact that the requester was so knowledgeable about what had been on the Web site and what had been removed. And national publicity did not hurt.[95] Other public interest groups are similarly situated to be agency watchers and request electronic copies of information removed from the Internet to be hosted on their own servers.

FOIA REQUESTS FOR INFORMATION IN AGENCY DATABASES

Public interest groups have long advocated for access to information in government databases so that the information can be made available to more people or be made available in a more user-friendly and meaningful format. An example of a public interest group that has taken information from disparate sources and made it accessible in a number of more useful formats is the OMBWatch and its RTKNET, a searchable environmental database that allows a user to aggregate information from numerous sources by geographic location, industry, or facility.[96] OBMWatch was recently successful in forcing RMP executive summaries to be released in an online format in compliance with the E-FOIA, and this information is now part of RTKNET.[97]

Carl Malamud, of public.resource.org, has been committed to providing public access to government information, from forcing the SEC to host the EDGAR database that he created to posting California's building codes online.[98] He is a huge advocate for more data being published by the government in an unstructured form so that agencies and third parties can find new ways to present it in ways that are meaningful to the public. Government information, even when available, is often not searchable in a useful manner. A few examples of these Web sites, or mash ups, that have taken government information and made it searchable in ways that are more informative include StateMaster's aggregation of statistical information that can be cross-searched and aggregated in visual maps, Follow The Money, a "database of state-level campaign contributions, searchable by candidate, contributor, office and state,"and Every Block.com, a mash up of municipal data that lets you find out what's going on near your house in 11 cities.[99] Carl Malamud has spearheaded the movement to allow the public to manipulate government data in ways that promote transparency when the government won't.

Malamud's method is pro-active, requesting or harvesting government information and then posting it for dedicated programmers to configure in useful ways, but the FOIA can also be used to request huge libraries of data. The E-FOIA expressly overrode:

> the holding in Dismukes v. Department of the Interior, that an agency "has no obligation under the FOIA to accommodate plaintiff's preference [but] need only provide responsive, nonexempt information in a reasonably accessible form." This precedent, which has been followed in at least one subsequent case, see Baizer v. U.S. Department of the Air Force . . . presents a reason for Congress to enact legislation to clarify the rights of requesters with respect to the form and format of the released record.[100]

The E-FOIA requires an agency to try and provide materials in any format requested and to make a reasonable search of computerized documents.[101] The E-FOIA also expressly rejected any definition of agency record that would exclude records that are "library material," as happened in *SDC Development Corp. v. Mathews*, where the court found that an agency-created computer database of research abstracts was not an agency record because it was library material beyond the reach of FOIA.[102] The information at issue in *Mathews* was the National Library of Medicine's MEDLARS database of stored and indexed medical bibliographic data. The information was available

only through subscription or purchase. A current FOIA request for a similar database of information would have to be honored pursuant to the express mandate of Congress in passing the E-FOIA.

Public.resourc.org made a similar request for "bulk access to the copyright catalog of monographs, documents, and serials on the Internet," also available for purchase at a significant cost.[103] The Copyright Office agreed that the information was in the public domain and could be harvested by anyone from its Web site.[104] There may be many sources of agency information where having the information provided in an open source format would make accuracy, manipulation, and reconfiguration easier. While the first resort would be to request the information and have the agency voluntarily provide it, as has been the case for the municipal information requested by EveryBlock,[105] if an agency is not forthcoming, a FOIA request may be an appropriate method to extract the information. An agency would have to provide open source data if it is not burdensome to do so, as the Senate made clear is passing the E-FOIA.[106]

The public's right to request a copy of the digital basemap information for Santa Clara County's parcel map information under California's Public Records Act was just upheld in *County of Santa Clara v. Superior Court.*[107] The map had been available only for purchase for very high fees. After the lawsuit was filed, the Department of Homeland Security designated the basemap protected critical infrastructure information, but the court of appeal rejected the designation, holding that the public interest in having access to the information outweighed the alleged national security interest left (after all, the basemap had been sold to at least 18 different customers).[108] This is a victory for open source data requests.

THE BALANCING ACT

Agencies have been and continue to be unprepared to deal with the requirements of E-FOIA.[109] 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."[110] 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. Non-profit organizations and their supporters are well-situated to challenge the removal of documents from the Internet and the current administration's shifting of the burden of producing documents.

Organizations such as the American Federation of Scientists, Project on Open Government, the National Security Archive, OMBWatch, and individual scholars and citizens have uncovered massive amounts of information the government might have wished to keep secret. 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 to accomplish openness in government. But it has always needed the actions of concerned citizens to keep it vital.

NOTES

1. *http://archive.org.*
2. 44 U.S.C. §§ 3301-3303a, 3308-3311 (2000). *See* US Dep't of Educ., Federal Records Act (FRA), *http://www.ed.gov/policy/gen/leg/fra.html* (last visited Jul 29, 2008); Armstrong v. Executive Office of the President, Office of Admin., 1 F.3d 1274, 1282-1283 (C.A.D.C. 1993) (noting that electronic communications systems can and have created documents that are federal records under the FRA that can be disposed of only pursuant to the FRA).
3. *See* Cottone v. Reno, 193 F.3d 550, 554 (D.C. Cir. 1999).
4. Older versions can usually be viewed at the Wayback Machine (*http://archive.org*). The Cybercemetary, at *http://govinfo.library.unt.edu/*, is where the Web sites of defunct agencies and commissions go to rest.
5. 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* (RAND Report); *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) (Emerging Threats hearings), available at *http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname'109_house_hearings&docid'f:20922.wais* (prepared statement by Thomas S. Blanton).
6. "Center Sues FERC Over Restricted Energy Information," Dec. 13, 2004, *http://www.ombwatch.org/article/articleview/2567/1/306.*
7. Emerging Threats hearings, *supra* n.5, at 110.
8. 5 U.S.C. § 552 (Supp. 2002).
9. OMB Watch has a detailed list of missing pages. "OMB Watch, Access to Government Information Post September 11th," *http://www.ombwatch.org/article/articleview/213/1/104* (last visited Oct. 26, 2005).
10. The following notice had been 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). This link is no longer available; a copy of the Web page is on file with the author. RMPs are still unavailable online, and the current EPA Web page states: "RMP information may be accessed via the Federal Reading Rooms . . . Federal Reading Rooms are open and available to the public to review RMP information." *http://www.epa.gov/OEM/content/rmp/index.htm#accessing* (last visited Sept. 1, 2008).
11. Paul M. Schoenhard, Note, "Disclosure of Government Information Online: A New Approach From an Existing Framework," 15 *Harv. J.L. & Tech.* 497, 518-519 (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). That period has been extended and regulations have been promulgated for paper distribution of most OCA materials. 40 C.F.R. §§ 1400.3; 1400.5).

12. 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 is supposed to be available on the Internet.
13. *See* OMB Watch, "Attack on Risk Management Plans," Sept. 30, 2001, *http://www.ombwatch.org/article/articleview/401/1/254?TopicID'1*, last visited Sept. 1, 2008.
14. 42 U.S.C. § 11023(j) (2006). *See* Brad Schweiger, "Safety vs. Security: How Broad but Selective Public Access to Environmental Data Properly Balances Communities' Safety and Homeland Security," 25 *John Marshall J. of Computer and Information Law* 273, 274 (2008), for a discussion of the increase in TRI reporting requirements since 1986 and the decrease, both in online access and in the number of facility reporting requirements, since 2001.
15. *See* U.S. Environmental Protection Agency, Accessing the Envirofacts Database, *http://www.epa.gov/enviro/html/technical.html#Accessing* (last visited Sept. 14, 2008); *and see* OMB Watch, *supra* n.31, *http://www.ombwatch.org/article/articleview/213/1/1/#EPA* (no direct access to Envirofacts Databases).
16. *See* 40 C.F.R. § 372.27 (Dec. 22, 2006), which increased the reporting threshold to 5,000 pounds. It was previously 500 pounds. 40 C.F.R. § 372.27 (June 26, 2000).
17. Designation under Executive Order 12958, 67 Fed. Reg. 31, 109 (May 6, 2002).
18. *Supra* n.5, at 86.
19. Union of Concerned Scientists, "Interference at the EPA: Science and Politics at the U.S. Environmental Protection Agency" (Interference at the EPA), Jul. 2008, *http://www.ucsusa.org/assets/documents/scientific_integrity/interference-at-the-epa.pdf*.
20. *Id.* at 33.
21. Political interference has always been an issue at the EPA, but according to the report, the severity of the problem has increased significantly over the past five years. *Id.* at 36.
22. *Id.* at 33.
23. EPA, State of Knowledge, *http://www.epa.gov/climatechange/science/stateofknowledge.html*, last accessed Sept. 14, 2008.
24. "Interference at the EPA," *supra* n.19, at 24. Two hundred tweny-nine scientists reported this problem. *Id.*
25. Brad Johnson, "Bush Hiding Truth: Global Warming Regulations Worth $2 Trillion Benefit" (Bush Hiding Truth), the Wonk Room, *http://thinkprogress.org/wonkroom/2008/06/30/bush-epa-suppression/*, June 30, 2008. The Office of Management & Budget refused to open the email that the EPA sent. The document has now been seriously revised. Julie Eilperin and R. Jeffrey Smith, "EPA Won't Act on Emissions This Year: Instead of New Rules, More Comment Sought," *Wash. Post*, July 11, 2008, at A1, also available at *http://www.washingtonpost.com/wp-dyn/content/story/2008/07/11/ST2008071100041.html*. The revised draft has been designated as an "Advance Notice of Proposed Rulemaking: Regulating Greenhouse Gas Emissions Under the Clean Air Act," *http://www.epa.gov/climatechange/anpr.html*, accessed on Sept. 15, 2008. On that date the comment period was still open.
26. Regulating Greenhouse Gas Emissions Under the Clean Air Act, 5-30-2008 Draft, at 93; the first 150 pages of the draft are available at *http://thinkprogress.org/wonkroom/wp-content/uploads/2008/06/anprm-may-30-draft-pp-1-75.PDF* and *http://thinkprogress.org/wonkroom/wp-content/uploads/2008/06/anprm-may-30-draft-pp-76-150.PDF*.
27. OMB Watch, Access to Government Information Post September 11th, *http://www.ombwatch.org/node/182*, last visited Feb. 12, 2009).
28. Electronic CEII & FOIA Request Forms, *http://www.ferc.gov/legal/ceii-foia.asp*, accessed Sept. 15, 2008.
29. Critical Energy Infrastructure Information General Non-disclosure Agreement, *http://www.ferc.gov/legal/ceii-foia/ceii/gen-nda.pdf*.
30. *Id.*
31. Critical Energy Infrastructure Information Regulations, Order No. 702, Oct. 30, 2007, *http://www.ferc.gov/legal/maj-ord-reg/land-docs/ceii-rule.asp*.
32. *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" (Keeping Secrets), *U.S. News & World Rep.*, Dec. 22, 2003, at 18, 20, 22, available at *http://www.usnews.com/usnews/news/articles/031222/22secrecy.htm*; "Now: Veil of Secrecy" (PBS television broadcast Dec. 12, 2003) (transcript available at *http://www.pbs.org/now/transcript/transcript246_full.html*). "Center Sues FERC Over Restricted Energy Information," *supra* n. 6.
33. "Keeping Secrets," *supra* n.32, at 22, 24, 25, 27, and 28.
34. *Id.*
35. *Id.*
36. *Id.*
37. The lawsuit seeks "copies of all documents in your custody or under your control related to correspondence, including but not limited to meetings, transcripts, schedules, minutes, and/or agendas between the Federal Energy Regulatory Commission and companies considering construction of liquefied natural gas facilities . . . ." Center for Public Integrity v. Federal Energy Regulatory Commission, Complaint for Declaratory and Injunctive Relief, 1:04cv2112-EGS, D.C.C., filed Dec. 6, 2004. Available though PACER.
38. "Center Sues FERC Over Restricted Energy Information," *supra* n.32.
39. Kevin Bogardus, "Appealing to a Higher Authority: Federal Energy Regulators Smooth the Way for Liquefied Natural Gas Terminals," Center for Public Integrity, Dec. 7, 2004, *http://store.publicintegrity.org/oil/report.aspx?aid=430&sid=100*.
40. *See, e.g.*, Doe v. Gonzales, 500 F. Supp. 2d 379, 421 (S.D.N.Y. 2007).
41. DOT, NPMS Data Security, *http://www.npms.phmsa.dot.gov/application.asp?tact'npms&page'subapp.asp?app'aboutnpms&act'public*: "The terrorist attacks of September 11, 2001 placed additional security concerns on the U.S. pipeline infrastructure. As a result, the Pipeline and Hazardous Materials Safety Administration restricts access to the NPMS to federal, state, and local government agencies (including emergency responders)."
42. DOT, About the NPMS Public Map Viewer, *http://www.npms.phmsa.dot.gov/application.asp?tact'npms&page'subapp.asp?app'aboutnpms&act'public*. The Public Map View is available at *http://www.npms.phmsa.dot.gov/*.
43. *See* n.27 *supra*. *See also* the RAND Report, *supra* n.5, at 171. These DOT databases were two of four out of 629 examined in the RAND Report that might have a medium significance to terrorists because of specificity of information and difficulty of accessing the information elsewhere. The RAND Report ranked this information "conservatively an using the limited information describing these databases caused us to classify them as medium significance. However, we were unable to examine these databases directly because of password restriction so an extensive evaluation might change such a ranking."
44. Pipeline Infrastructure Protection to Enhance Security and Safety Act, 2001, Cong. H.R. 3609 (Dec. 20, 2001). The bill would have amended 49 U.S.C. § 60117.
45. "Army Blocks Public Access to Digital Library," Feb. 13, 2008, *http://www.fas.org/blog/secrecy/2008/02/army_blocks_public_access_to_d.html*.
46. *Id.*
47. "The Reimer Digital Library is Back," *Secrecy News*, Mar. 6, 2008, *http://www.fas.org/blog/secrecy/2008/03/the_reimer_digital_library_is_.html*. Every document may not be back in an accessible form. A few can't be accessed, although clearly marked "approved for public release; distribution is unlimited." *Id.* An example of such a document has been posted by Secrecy News at *http://www.fas.org/irp/doddir/army/fmi3-04-155.pdf*.
48. "Marine Corps Will Restore Online Access to Public Documents," Secrecy News, Mar. 27, 2008, *http://www.fas.org/blog/secrecy/2008/03/marine_corps_will_restore_online_access_to_public_documents.html*.
49. "Orders & Directives: Doctrinal Pubs," Marine Corps, *http://www.marines.mil/news/publications/Pages/order_type_doctrine.aspx*, accessed on Sept. 27, 2008. FAS also hosts a selection of US Marine Corps doctrinal publications at *http://www.fas.org/irp/doddir/usmc/index.html*.

50. "Small Business Advocates Want Contract Data Back on Website," *Miami Herald*, Dec. 16, 2006, *http://www.miami.com/mld/miamiherald/business/16251795.htm*.

51. *Id.*

52. Democratic Staff of H. Comm. on Small Business, Scorecard VII: Faulty Accounting by Administration Results in Missed Opportunities for Small Businesses, July 26, 2006, *http://www.house.gov/smbiz/Reports/ScoreCardVIIFINAL.pdf*.

53. American Small Business League v. SBA, No. 08-00829MHP, memorandum & order Re: Motion for Summary Judgment, Aug. 28, 2008, *http://www.asbl.com/documents/20080925courtordermod.pdf*, at 2.

54. *Id.* at 5-6.

55. "SBA Appeals Federal Court Ruling to Release Contracting Data: SBA Moves to Limit Public Access to Contracting Data," *MarketWatch.com*, Sept. 25, 2008, *http://www.marketwatch.com/news/story/sba-appeals-federal-court-ruling/story.aspx?guid'%7BC7D038E7-AFC3-4732-BC44-68EF12A0CEF6%7D&dist'hppr*.

56. Brenda Wilson, "Health Database Blocked Searches on 'Abortion,'" NPR, Apr. 4, 2008, *http://www.npr.org/templates/story/story.php?storyId'89398211*.

57. *Id.*

58. Brenda Wilson, "Magazine Led to Database's 'Abortion' Search Block," Apr. 9, 2008, *http://www.npr.org/templates/story/story.php?storyId'89486048*.

59. "Classified Letters Regarding FBI Whistleblower Sibel Edmonds," *http://www.thememoryhole.org/spy/edmonds_letters.htm* (last visited Sept. 27, 2008); 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*.

60. *Id.*

61. Stipulation of Dismissal, Project on Gov't Oversight v. Ashcroft, Civ. No.1:04cv1032 (D.C. Cir. Mar. 9, 2004), *http://www.citizen.org/documents/stipdismissalasfiled.pdf*; *see also* Letter of Vesper Mei, US 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").

62. Linda-Jo Schierow, Congressional Research Serv., Chemical Plant Security 12 (CRS Report No. RL31530, 2005). Just walking around would give terrorists detailed information of the kind needed to plan an attack, but not available in RMPs,which provide only the more general information needed to identify a site) *id. See also* Linda-Jo Schierow, Congressional Research Serv., Chemical Plant Security 12 -14 (CRS Report No. RL31530, 2006), documenting later investigations.

63. *Id.*

64. The RAND Report, *supra* n.5, at 100-103.

65. *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.*

66. *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.").

67. *Id. at* 69, 70.

68. Emerging Threats hearings, *supra* n.3, at 100. Erwin Griswold, who was the Solicitor General of the United States in the 1970s and the counsel for the United States in its efforts to suppress the Pentagon Papers, had this to say about excessive secrecy: "It quickly becomes apparent to any person who has considerable experience with classified material that there is massive overclassification and that the principal concern of the classifiers is not with national security, but with governmental embarrassment of one sort or another." "Secrets Not Worth Keeping: The Courts and Classified Information," *Wash. Post*, Feb. 15, 1989, at A25.

69. Amanda Fitzsimmons, "National Security or Unnecessary Secrecy? Restricting Exemption 1 to Prohibit Reclassification of Information Already in the Public Domain," 4 I/S: *J. L. & Pol'y for Info. Soc'y* 479, 504, 505 (2008).

70. 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*; 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*.

71. Press Release, "Memorandum for the Heads of Executive Departments and Agencies (Subject: Freedom of Information Act), Jan. 29, 2009.

72. *OpenTheGovernment.org*, Secrecy Report Card 2008: Indicators of Secrecy in the Federal Government 10, *http://www.openthegovernment.org/otg/SecrecyReportCard08.pdf*, accessed Sept. 29, 2008.

73. *Id.*

74. Project on Government Oversight v. Ashcroft, 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*.

75. Cottone v. Reno, 193 F.3d at 554, *supra* 3 (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); Davis v. United States 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.").

76. *See generally* 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, 131 (2003), citing United States v. Heine, 151 F.2d 813 (2d Cir. 1945); United States v. Truong, 629 F.2d 908, 918 n.9 (4th Cir. 1980); and Slack v. United States, 203 F.2d 152, 156 (6th Cir. 1953).

77. Afshar v. Department of State, 702 F.2d 1125, 1130 (D.C. Cir. 1983).

78. The Public's Domain, *supra* n.81, at 123.

79. Exec. Order No. 13,292, 68 Fed. Reg. 15,315 (Mar. 25, 2003), amending Exec. Order No. 12,958, 60 Fed. Reg. 19,825 (Apr. 17, 1995).

80. Schoenhard, *supra* n.13, at 51314 (citing Founding Church of Scientology v. NSA, 610 F.2d 824, 831, 832 (D.C. Cir. 1979).

81. P.L. 104-231, 110 Stat. 3048 (1996).

82. 5 U.S.C. § 552(a)(2)(D), (E) (2000); 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); 5 U.S.C. § 552(f)(2) (2000).

83. 5 U.S.C. § 552(a)(3)(B) (2000); 5 U.S.C. § 552(a)(2)(D) (2000). *See also* 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. 2, 2008).

84. 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*.

85. *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).

86. 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 an excellent overview of the Act's requirements).

87. Minority Staff, Comm. on Gov't Reform, U.S. House of Representatives, Secrecy in the Bush Administration 4, 30-31 (2004).

88. 5 U.S.C. § 552(a)(2)(D) (2000).

89. 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. 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.gao.gov/new.items/d02493.pdf*.

90. For a list of agency regulations, *see* Susan Nevelow Mart, "Let the People Know the Facts: Can Government Information Removed From the Internet Be Reclaimed?," *http://www.llrx.com/features/reclaimed.htm#appendixtwo*, visited Oct. 4, 2008.
91. H.R. Rep. No. 104-795, at 11 (1996), *reprinted in* 1996 U.S.C.C.A.N. 3448, 3454.
92. Reporters' Comm. for Freedom of the Press, FOI Letter Generator, *http://www.rcfp.org/foi_letter/generate.php* (last visited Oct. 4, 2008). A similar form could be created by any public interest group seeking to have interested parties make multiple FOIA requests.
93. A copy of the FAS FOIA request for the Reimer Library digital documents is available at *http://www.fas.org/sgp/news/2008/02/reimer.pdf*; a copy of the FAS FOIA request for the Marine Corps digital doctrinal documents is available at *http://www.fas.org/sgp/news/2008/03/usmc-doctrine.pdf*.
94. "Army Blocks Public Access to Digital Library," *Secrecy News*, Feb. 13, 2008, *http://www.fas.org/blog/secrecy/2008/02/army_blocks_public_access_to_d.html*.
95. "Army Blocks Public's Access to Documents in Web-Based Library," *Wash. Post*, Feb. 21, 2008, at A13, available at *http://www.washingtonpost.com/wp-dyn/content/article/2008/02/20/AR2008022002830.html*.
96. *http://www.rtknet.org/*.
97. "OMB Watch Wins in Court for Access to Risk Management Data," July 11, 2005, *http://www.ombwatch.org/article/articleview/2915/1/242?TopicID'1*, last visited on Sept. 1, 2008. The law requires that "RMP reports be collected and released to the public and that reading rooms around the country provide access to paper versions of the documents. The appeal also pointed out that under the Electronic Freedom of Information Act Amendments, agencies may not deny requests for electronic format if the information is releasable. After waiting for almost two years for EPA to respond to the appeal, OMB Watch retained legal counsel and filed a complaint. After only 30 days, the agency provided the data without ever filing a counter-argument or offering an explanation for its early refusals."
98. See "About Carl Malamud," *OnTheCommons.org*, *http://onthecommons.org/profile.php?id=1994* (last visited Oct. 4, 2008).
99. *http://www.statemaster.org*: "Welcome to StateMaster, a unique statistical database which allows you to research and compare a multitude of different data on US states. We have compiled information from various primary sources such as the US Census Bureau, the FBI, and the National Center for Educational Statistics. More than just a mere collection of various data, StateMaster goes beyond the numbers to provide you with visualization technology like pie charts, maps, graphs and scatterplots. We also have thousands of map and flag images, state profiles, and correlations."
100. S. Rep. 104-272, at 14-15.
101. *Id.* at 22.
102. H. Rep. 104-795, at 20, citing SDC Development Corp. v. Mathews, 542 F.2d 1116 (9th Cir. 1976).
103. Letter to the Honorable Marybeth Peters, US Register of Copyrights, from a consortium of public interest groups, Sept. 17, 2007, *http://public.resource.org/copyright.gov/index.html*.
104. Letter to Carl Malamud from the Registrar of Copyrights, Oct. 18, 2008, *http://public.resource.org/scribd/3319365.pdf*.
105. Speech given by Daniel X. O'Neil, Mar. 19, 2008.
106. S. Rep. 104-272, at 14-15. The report notes that the "requirement to make records available in the form or format requested by any person where such records are not usually maintained in the requested form or format, is subject to a 'reasonable efforts' qualification . . . This requirement applies to choices between conventional record forms (e.g., paper, microfiche, or electronic) as well as to choices between existing electronic formats."
107. County of Santa Clara v. Superior Court, No. H031658, Feb. 5, 2009, *http://www.courtinfo.ca.gov/opinions/documents/H031658.PDF*.
108. Pete Scheer, "In Far-reaching Decision, Appeals Court Affirms Public's Right to County Mapping Database," Cal. First Amendment Coaltion, Feb. 6, 2009, *http://www.cfac.org/content/index.php/cfac-news/legal_development/*.
109. Michael Tankersley, "How the Electronic Freedom of Information Act Amendments of 1996 Update Public Access For the Information Age," 50 *Admin. L. Rev.* 421, 428-29 (1998).
110. Memorandum from Richard L. Huff & Daniel J. Metcalfe, Co-Directors, Office of Information and Privacy, US 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*.