Access to Information after 9/11

Lee Tien

Senior Staff Attorney
Electronic Frontier Foundation
www.eff.org

Overview

Public access to information held by government has long been a contentious issue. Proponents of government secrecy have traditionally argued that public access interferes with the government's internal decision-making processes, imposes costly burdens on agencies, and makes private companies unwilling to share information with the government.

These complaints have only grown louder since September 11. The Bush administration has shown on a number of fronts that it values secrecy more than accountability: it has shifted its information policy away from public access and has taken unprecedented steps to "depublish" information on government websites. And Congress is now considering whether to protect companies' voluntarily submitted "cybersecurity" or "critical infrastructure" information against public access on the theory that secrecy is necessary in order to induce private firms to cooperate with the government.

EFF believes that such concerns are overblown. As a legal matter, the federal statutes that protect the public's right to know already contain exemptions can adequately protected such information. More important, security vulnerabilities are clearly of great importance to the public — infrastructure is critical precisely because we all depend on it. If companies are allowed to shield information about the risks in their systems, there cannot be meaningful public discourse about those risks or the measures taken to address them.

Statutory background

The two main federal disclosure statutes are the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and the Federal Advisory Committee Act (FACA), 5 U.S.C.App. § 2 (Pub. L. No. 92-463, 86 Stat. 770 (1972)).

Both statutes protect the public's interest in accountability by restricting government secrecy. Under FOIA, agency records must be provided to any person on request unless one of several exemptions applies. The purpose of FOIA is "to open agency action to the light of public scrutiny," so that citizens can know "what their government is up to." *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 772, 773 (1989). If an agency fails to comply with FOIA, the requester may file a civil lawsuit to compel its disclosure, and may receive attorney fees and costs if he or she substantially prevails in court.

The FACA generally controls the advisory committee process and was enacted "to open to public scrutiny the manner in which government agencies obtain advice from private individuals." *Nat'l Anti-Hunger Coalition v. Executive Comm. of the President's Private Sector Survey on Cost Control*, 711 F.2d 1071, 1072 (D.C. Cir. 1983); *see also Pub. Citizen v. U.S. Dep't of Justice*, 491 U.S. 440, 459 (1989). FACA was intended to protect against undue influence by special interest groups. H.R. Rep. No. 92-1017, at 4 (1972); S. Rep. No. 92-1098, at 3-6 (1972).

Bush administration policy on FOIA requests

The Department of Justice recently shifted its policy emphasis for FOIA requests. The Clinton administration's policy was to release information unless it was "reasonably foreseeable that disclosure would be harmful." Attorney General Janet Reno declared a presumption of "maximum responsible disclosure of information." Because the "American public's understanding of the workings of its government is a cornerstone of our democracy," the government "must ensure that the principle of openness in government is applied in each and every disclosure and nondisclosure decision that is required under the Act."

Attorney General John Ashcroft's October 12 memo on FOIA implementation sounds a different chord. (http://www.usdoj.gov/oip/foiapost/2001foiapost19htm) As Harry Hammitt of *Access Reports* notes, "the tone of Ashcroft's memo is protection of information." *Access Reports*, vol. 27, no. 20 (Oct. 24, 2001) (http://www.accessreports.com).

Hammitt points out that the Reno and Ashcroft memos differ greatly in their attitude toward Exemption 5 of the FOIA, which is often used to shield "deliberative" inter-agency and intra-agency materials against disclosure in order to protect the government's interest in candid discussions. As Hammitt puts it, "Reno urged agencies to maximize disclosure of internal memos by withholding information only when there was a foreseeable harm that would flow from disclosure." In contrast, the Ashcroft memo states that when agencies "decide to withhold records, in whole or in part . . . the Department of Justice will defend [the] decisions unless they lack a sound legal basis or present an unwarranted risk of adverse impact on the ability of other agencies to protect important records."

It is difficult to say how much a difference this policy shift will make. But Vice-President Dick Cheney refusal to release records of his energy task force is certainly suggestive. The General Accounting Office's lawsuit against Cheney has gotten much press, but the GAO is not alone in seeking task force records: Judicial Watch has filed a FACA suit; the Natural Resources Defense Council has filed a FOIA suit; the Sierra Club has filed another FACA suit in California.

Notably, when Judicial Watch got its first hearing, U.S. District Judge Emmet Sullivan ordered the government to preserve the task force records and told the government attorneys: "I don't think the government is taking this case seriously. You say there's no factual dispute in this case just because you say there's no factual dispute. . . . That's an incredible statement." *Access Reports*, vol. 28, no. 3 (Feb. 13, 2002).

Similarly, U.S. District Judge Kessler recently ordered DOE to release the "vast majority" of the documents requested by NRDC by March 25, 2002. In her opinion, Judge Kessler called DOE's initial response to NRDC "virtually meaningless." She found that DOE had "no legal, or practical, justification for working at a glacial pace" to fulfill NRDC's request, noting that "[i]t is very hard to discern … what in the world Department personnel were doing from July 2001 through December 2001 when they were conducting 'periodic' reviews of the 2,149 documents (comprising 7,584 pages) deemed responsive to the request." The judge added, "the material which [NRDC] seeks is of extraordinary public interest. The subject of energy policy, especially since the terrible events of September 11, 2001, is of enormous concern to consumers, to environmentalists, to the Congress, and to industry." (http://www.nrdc.org/media/default.asp#0227taskforce)

Government restrictions on information publication

Another sign of the Bush administration's attitude toward access is the steady removal of formerly public information from government websites. In January, the administration "began quietly withdrawing from public release more than 6,600 technical documents that deal mainly with the production of germ and chemical weapons. It is also drafting a new information security policy . . . that officials say will result in more documents' being withdrawn." William Broad, "U.S. Tightening Rules on Keeping Scientific Secrets," *The New York Times* (Feb. 17, 2002) (http://www.nytimes.com/2002/02/17/politics/17SECR.html). The withdrawn documents had all been freely sold to the public; some had undergone modern review for declassification.

But the Bush policy goes beyond removing information from the public domain. According to the *Times*, the government has asked the American Society of Microbiology "to limit potentially dangerous information in the 11 journals it publishes." One proposal reportedly being debated at the National Academy of Sciences is "to eliminate the sections of articles that give experimental details researchers from other laboratories would need to replicate the claimed results, helping to prove their validity."

More generally, many agencies have been removing information from their websites and providing only limited access to select entities. Among them are: the Department of Energy; the Environmental Protection Agency; the Federal Aviation Administration; NASA; the Department of Transportation; and the U.S. Geological Survey. OMB Watch is tracking these removals on its website. (http://www.ombwatch.org/info/2001/access.html)

In one well-publicized incident, the Superintendent of Documents of the Government Printing Office in October 2001 requested Federal depository libraries to withdraw from public circulation and destroy their depository copies of a U.S. Geological Survey CD-ROM ("Source Area Characteristics of Large Public Surface-Water Supplies in the Conterminous United States: An Information Resource for Source-Water Assessment, 1999") providing information on water resources. In a statement issued January 16, 2002, the GPO explained that the request was made on behalf of the USGS. When asked if this action was necessary, a USGS e-mail dated October 31, 2001, said: "Subsequent contact with the Government Printing Office and the USGS Committee that sets official policy on restriction of sensitive information has reconfirmed the validity of the original written instruction from USGS and GPO to destroy the report."

The federal government is not alone. States like New York, New Jersey, Pennsylvania and Florida are also removing from websites or restricting access to formerly public information. OMB Watch is tracking these restrictions as well.

Case study: cybersecurity information

The Cyber Security Information Act (CSIA) (H.R. 2435) would protect the confidentiality of "cyber security information" submitted voluntarily by private firms. The Critical Infrastructure Information Security Act of 2001 (CIISA) (S. 1456) would protect the confidentiality of voluntarily submitted "critical infrastructure information," which is defined so broadly as to include information about virtually every possible weakness in our "critical infrastructure," from telecommunications to banking.

Whether any new protection is needed for such information is dubious. Government vulnerability assessments are generally exempt from public disclosure under the (b)(2) FOIA exemption. Meanwhile, existing FOIA exemptions generally protect voluntarily submitted trade secrets or other valuable business information. *See Critical Mass Energy Project v. Nuclear Regulatory Commn*, 975 F.2d 871, 880 (D.C. Cir. 1992) (en banc), *cert denied*, 507 U.S. 984 (1993) (discussing the (b)(4) FOIA exemption). Government officials have stated that existing FOIA law need not be changed in order to protect voluntary private sector submissions.

Indeed, a recent letter from industry groups concedes that existing FOIA case law "suggests that a federal agency would win a test case." But they argue that "the risk of a loss of such a test case – as viewed by the parties bearing the risk – remains unacceptably high. More importantly, corporations should not be required to accept such risks, or the cost of litigation, when reporting significant cyber events in an attempt to protect the public interest."

Unfortunately, President Bush has already stated in a letter to the chair of the National Security Telecommunications Advisory Committee that his administration will "support a narrowly crafted exception (to the Freedom of Information Act) to protect information about corporations' and other organizations vulnerabilities to information warfare and malicious hacking."

But the issues raised by these bills go beyond the mere availability of FOIA or FACA. For instance, the bills also limit other kinds of disclosure and use of such "voluntarily submitted" information by the government and other parties without the submitter's express permission. Under CSIA, covered information "shall not be disclosed to any third party," subject to narrow exemptions. § 4(c)(2). Moreover, such information "shall not be used" by anyone, "directly or indirectly, in any civil action." § 4(c)(3). CIISA contains similar, although slightly narrower, provisions. §§ 5(a)(1)(B), (C).

The larger issue is the purported trade-off between security and public disclosure. Industry argues that we must generally suppress information about security weaknesses in order to prevent some people (maybe terrorists) from attacking those weaknesses.

But this approach hardly justifies a FOIA exemption. After all, how many attackers bent on terrorism are going to file FOIA requests for this kind of information in the first place? Or litigate agency denials in federal court? Even garden-variety FOIA requests can take years to process simply because of FOIA backlogs. It's far more likely that potential attackers would discover or develop information about such weaknesses themselves. If so, then a proposed FOIA exemption isn't really about terrorism at all.

What is it about? The approach focuses on knowledge about the weaknesses — not the weaknesses themselves. It leaves the public in the dark about the vulnerabilities of the systems they use or depend on, thus stifling public discourse about those vulnerabilities. The obvious result: it's harder to hold companies accountable for the security weaknesses of their products or services.

As James Dempsey of the Center for Democracy and Technology has said, "for some security vulnerabilities, we need more exposure, not less. It's the only way things are going to be fixed." Without public disclosure, he added, "The question of what did they know and when did they know it

can never be asked."

A classic example is the March 1997 publication by security researcher David Wagner, now a professor at UC-Berkeley, of flaws in the privacy codes used by U.S. digital cellular phones used by tens of millions of U.S. citizens. This work not only received widespread news coverage (e.g., the front page of the New York Times), but also helped convince the U.S. cellular standard committee to undertake a sweeping re-design of their security architecture.

There's good reason to think that this closed-meeting approach to security is just plain bad for security. Security research is a collaborative discipline. In the area of cryptography, for instance, experience has shown that many encryption systems have unexpected flaws when first propoosed. What one researcher may overlook, a fresh set of eyes may discover.

At the same time, security is also an adversarial discipline. One must think like an attacker in order to anticipate how one's own security system might be attacked. Cryptographer Bruce Schneier has put it more colorfully:

"Cheating is one of the basic tenets of security engineering. Conventional engineering is about making things work. . . . Security is different; it's about making sure things don't NOT work. It's making sure security isn't broken, even in the presence of a malicious adversary who does everything in his power to make sure that things don't work in the worst possible way at the worst possible times. A good attack is one that the engineers never even thought about. Good attackers cheat."

Thus, in the security field, vulnerability information has legitimate uses. Security is truly enhanced by fixing known weaknesses and testing for potential weaknesses. It's doubtful whether CSIA and CIISA would make this more likely.

Resources

Access Reports, http://www.accessreports.com
American Library Association, http://www.ala.org/washoff/righttoknow.html
Federation of American Scientists' Project on Government Secrecy, http://www.fas.org/sgp/index.html
OMB Watch, http://www.ombwatch.org
Post Sept. 11 environment, http://www.ombwatch.org/info/2001/access.html