
“Access to Records” Versus “Access to Evil:” Should Disclosure Laws Consider Motives as a Barrier to Records Release?

Professor James T. O’Reilly

I. INTRODUCTION

The right of broad public access to government documents is a relatively recent American invention, a phenomenon that has spread onto the world stage in fits and starts.¹ The momentum supporting the “freedom of information” concept has been flowing in only one direction, toward greater transparency and greater dissemination of more government information, and this flow has been accelerated by the inexpensive technology for Internet posting of government documents. While it has never achieved constitutional status,² the right of access to most types of government records was a part of our national consensus from July 4, 1966, when the Freedom of Information Act was adopted,³ to September 11, 2001. Since then, something may have changed.

The attack on America may have been facilitated by the astute use of information readily accessible on the Internet. The images of military searches in Afghan caves were widely shown in the media and the terrorists may have uncovered information downloaded from American Web sources.⁴ Perhaps a climate change has occurred within government as a result. Has the tragic loss of lives on September 11 altered the world within which government disclosure about weaknesses was long perceived as a costless “free good”? Has the discovery within Al Qaeda’s control of U.S. infrastructure documents⁵ reduced the fervor for more and more openness of federal files? And what will

Professor O’Reilly teaches at the University of Cincinnati College of Law. He is the author of West’s Federal Information Disclosure (3d ed.) and 27 other textbooks. Professor O’Reilly chairs the ABA Committee on Government Information and Privacy and has been a federal consultant and witness on disclosure and privacy issues. He is a graduate of Boston College and the University of Virginia School of Law.

a new balance look like?

II. A BRIEF HISTORY OF OPEN ACCESS

Ordinarily, people are selective in their disclosures to others. People are reluctant to “tell all” to every neighbor, every banker or every retailer. The concept of individual private citizens being forced to disclose to “any person” any of the records, papers or recordings the private person makes, would be blatantly unconstitutional and roundly condemned by privacy advocates.⁶ Yet we have the opposite cultural expectation about the behavior of federal and state employees paid by tax funds to gather information, write analytical reports, conduct intelligence gathering, and plan major policy matters. We seem to have come to a quiet, implicit societal expectation that if the government touches (or could touch⁷) the record, it will be released to “any person” upon her or his request. Exceptions to this expectation exist⁸ and litigation may be required, but the cultural expectation persists that “government secrecy” is anathema. This paper surveys how Americans came to have such an “information entitlement,” an expectation of informational transparency, and then discusses how the tragedies of September 11, 2001, will change that expectation.

A. Freedom of Information Act

The U.S. Freedom of Information Act (FOIA) delivers access to federal files to “any person,” regardless of location, status, motive or interest.⁹ This simplistic “open to all” approach was a gift to the general populace from the newspaper editors’ lobbying group that successfully pressed the House and Senate to adopt FOIA over stern warnings from the Executive Branch. Though the statute empowers “any person” to request access, the original concept was that news media access needed to be enhanced by removing the news reporter’s chronic dependence upon “leaks” of government information.¹⁰ If information is a commodity, the newspaper lobby sought to gain more leverage over the delivery of that commodity. Change was needed to make it easier for investigative reporters to dig through stacks of paper to find publishable evidence of government employee misconduct. But the early hearings demonstrated that government employees would not act counter-intuitively and disclose all the records that would reveal their actions—not unless Congress forced them to do so.¹¹

So the very effective newspaper lobbyists invested in a campaign for “freedom of information,” a title of such nobility that it cannot be doubted. The vehicle for change was legislation altering the 1946 Administrative Procedure Act, which limited access to federal agency records to persons who could show they were “properly and

Motives and Information Disclosure Laws

directly concerned,” and allowed access only if no other legislation had required secrecy for that record. The 1946 law allowed the agency to keep records “confidential for good cause found” but did not provide a mechanism to enforce this discretionary option against an unwilling bureaucrat.¹²

Along with the press, other potent constituents jumped on the bandwagon for greater disclosure. Soon the merged interests of “insiders” in Washington and those of the press, as conditional “outsiders,”¹³ brought about the political pressure needed to overcome agency staff opposition to FOIA. The press wanted better access to what the bureaucrats knew and would selectively leak to favored journalists. The Washington law firms and the organized bar wanted a requirement that agency “secret law” policies must be codified and published, so as to facilitate the representation of more sophisticated clients in agency adjudicatory proceedings.¹⁴ Although the words “any person” appear in the text, this was not a reflection of any sponsor’s populist expectations that hundreds of thousands of individuals would demand access. Sponsors thought the costs would be small; they could not foresee that by fiscal year 2000, the federal government would be spending close to \$300 million on FOIA.¹⁵ A close reading of the committee process in the House and Senate shows that the bills were not a mass movement of the public demanding its rights. Instead, FOIA reflected the well-focused group desires of those whose daily trade was the retail sale of information and for whom access meant substantially greater empowerment in extracting more data for greater sales of their products.

B. Other Access Laws

The news media success with the adoption of a federal Freedom of Information Act led to equivalent legislation being adopted in virtually every state, some in the format of a complete statutory access package, and some as mere paragraph or page-long sections that were left to judicial interpretation. The state legislation was more likely to open the requester rights to “any person”¹⁶ or “any resident” or to put in a conditional phrase about a “concerned person,” like Virginia’s requirement that the requesters be “citizens of the Commonwealth,”¹⁷ and many followed FOIA federal model. For example, Ohio permits requests by “any person” but specifically limits access by “a person who is incarcerated pursuant to a criminal conviction or a juvenile adjudication.”¹⁸ California passed a specific statute allowing elected officials access to records “on the same basis as any other person.”¹⁹

The other nations that adopted such laws typically followed the “every person”²⁰ or “any person”²¹ model. Australia chose the “any person” model and specified that the motives of the requester were not to be considered.²² The European Union has struggled with these issues and in a 1990 Directive, provided environmental

information from public files to “any natural or legal person . . . without his having to ‘prove’ an interest.”²³ Other nations were not so generous. Canada limited access to its citizens and lawful residents.²⁴

While most other nations followed the template of the U.S. FOIA in allowing the unqualified term “any person,” they usually gave broader protection to governmental interests that underlie the exemption provisions of these statutes. FOIA was designed with nine narrow exemptions to be read quite narrowly. These cover trade secrets, classified military secrets, FBI informant data, etc. and are consciously less flexible and less broad than the looser exemptions used in other nations.

Law enforcement’s protection against disclosure is more clearly articulated outside the United States than it is in FOIA exemption 7, exempting “records or information compiled for law enforcement purposes.”²⁵ One can also see protections that balance access and secrecy within two categories, those of policy formation and those of commercial data. The former is a protection for parliamentary and political policy formation, a category of sensitive advice and recommendations that were often leaked to the press despite the desires of cabinet ministers. The latter is given more protection against disclosure in those nations where the business community actively participated in the statutory drafting debates, than in the United States, where FOIA passed with relatively little business input.²⁶

C. The “Right to Know” Movement

The reader should notice a significant difference between the quick and easy access to federal websites, and the costly and slow process for FOIA requests. The right to know could be manifest by acts of affirmative dissemination or by passive response to requests for existing documents. Affirmative dissemination by press release or otherwise is one style; another is to await the requests of persons who might have an interest or need for a topic. The trend toward affirmative dissemination means that a large mass of documents is to be placed on the Web without knowing who may use them for what purpose. This goes a step beyond the passive FOIA’s permission to any person to make a request,²⁷ for here, any person can obtain the records, leaving no paper trail to indicate that records on a subject had been downloaded by anyone.

The effort to enact U.S. “right to know” legislation was born 25 years ago, as a result of an incident that raised alarm among workers.²⁸ An insect infestation caused problems for U.S.-owned fruit companies operating in Central America, and so a U.S.-based chemical company developed the ideal chemical²⁹ to be sprayed on the banana trees. But in its concentrated form at the factory in California, the pesticide worked too well, causing plant workers to discover that they were far less able to have children than comparable-aged persons who worked elsewhere. The banana chemical’s

potency was a mystery to the workers—a mystery that led the head of the chemical workers to send a national warning to its members, calling on local chemical unions to insist on their “right to know” of health risks from chemicals used in the workplace.³⁰

From the banana incident came the coordinated chemical union thrust for mandates on employer disclosure of chemical risk to the affected workers. A disclosure norm that placed unionized plants at a disadvantage was deemed unacceptable, so legislative efforts led to governmental imposition of the disclosure commands. Two branches of this effort soon appeared: a worker-specific right to know of chemicals, which led to a final federal regulation applicable to all private sector workers with few exceptions;³¹ and a public and firefighter right to know of emergency response risks, which led ultimately to the 1986 Superfund Amendments and Reauthorization Act (SARA) Title III regarding public health emergencies³² and the 1990 Clean Air Act “risk management plan” requirements.³³

The present state of the industrial and commercial “right to know” is virtually the opposite of the world as it was just 25 years ago. In about a generation’s time, the world of industrial chemical use and production has moved from a secretive alchemy to a publicly posted overload of papers, training materials and neighborhood emergency maps. So people who enter the workforce or organize their neighborhoods today have tools of informational power that completely override the patterns as they were in the late 1960s. Information is power, and this is a significant shift of power.

As a result of empowerment through broader information dissemination concerning risks, a major philosophical shift has occurred. We have abandoned long-standing “government knows best” approaches to the handling of sensitive information. Before the right to know trend arose, privately generated information was a type of input to federal decisions, and private information was one component of a governmental decision process leading to regulatory adjudications. Citizens paid taxes; a share of the tax money was used to hire experts; career government experts monitored private activity, in some cases with information from private companies; and if a problem was found, the government took enforcement action. The public received the results but not the set of inputs. The paradigm was entirely consistent with a minimalist-access paradigm, since the decision flow was entirely into and then within government and the data entering government was exclusively beneficial to experts within the governmental body. Government agencies produced decisions, not data banks to be privately mined.

The new paradigm expects government agencies to be re-transmitters of incoming data, transparent tunnels through which the content of information is to be delivered to any reader or user who cares to download the data. The momentum for this new paradigm was growing rapidly before September 11, 2001.

III. WHERE THE NEW PARADIGM WOULD HAVE LED

As the agency Internet volumes expanded in the 1990-2003 period, policy debates about the merit of governmental disclosures diminished rapidly and the Internet postings seemed to be a “free good.” Transparency had a few detractors on the margin, but conflicts about the social benefit of disseminating private data through government vehicles such as FOIA or the Web were infrequent. There was such presumed benefit from transparency of government that a peaceful world could envision the day when websites for all agencies would serve the public through their library dissemination function, apart from their regulatory roles. By 2010 we probably would have seen “maximalist” information flows from regulated firms direct to the public, or through government agencies acting as libraries or as Webmasters for the posting of the information. For example, the real-time monitoring of stack gas contents within large smokestack emissions would produce a constant flow of data relevant to a company’s compliance with its Title V air pollution permit. In the future, the released gas figures would be accessible to the federal agency and the agency may have instantly posted these figures on its website or made them accessible in real time to anyone wishing to monitor the factory’s current contribution to today’s air quality in the neighborhood near the factory.

The vision of a truly transparent regulatory environment with extensive public access to information rejects past assumptions of minimalist dissemination of useful information to a limited set of government officials. The vision was accompanied by the signs of a remarkable change in enforcement modes. The number of active enforcement inspectors had always lagged behind the number of facilities to be regulated, sometimes by ten or a dozen or even a hundred facilities to one inspector. The data was in the files of the field offices of agencies, but they lacked sufficient resources to use the data effectively.

Private environmental litigants could obtain access to certain information from the alleged violators under discovery rules, but they often found the protective orders that accompanied discovery documents to inhibit the use of that data with broader audiences. But the citizen suit and the Web-based press criticism of private firms’ environmental conduct augmented the slow and steady pace of government agencies’ enforcement staffs. So these new modes of enforcement were fed by the broader public dissemination of the regulated facility’s data.

Where that experience of expanded transparency *would* have led us, remains mere speculation in light of the Sept. 11 attacks. American war efforts that center upon information and counter-information “weapons” inevitably affect the transparency of government. Disclosure tendencies are one victim of the unconventional terrorist war that we must defend, and in the absence of a battlefield

and a maneuvering army arrayed against us, the Internet is the visible sign of the enemy's movement against us. One of the early casualties of this war has been the campaign for full transparency of government files.

IV. THE ROLE OF THE PRESS

While the government information flow was changing and the enforcement vehicles were shifting, the press role also became quite dynamic. Information became "news" and then became "content," and the rush for more "content" reflected the pressure on media conglomerates like Rupert Murdoch's Fox networks. In the ancient 1980s, three or four media outlets for a smaller regional city, and eight or nine for a metropolitan area, might carry real news. The Freedom of Information Act was underutilized by journalists, though stories from government files were occasionally presented when disgruntled workers leaked information that led to a FOIA request. The press acted as a filter for the governmental data and for the health or environmental reports that governments reluctantly released to persistent reporters. A minimalist access regime released minimal information, except when it suited the agency's purposes to disseminate a piece of helpful information. The news media as a filter of government releases would occasionally find a gem, usually led to it by a disgruntled worker or competitor, but rarely would the news media dig through government files for a story. The quantity of stories about governments and risks of exposures was always finite, always capped by the limited number of news media reporters willing to derive printable stories from a mass of documents or reports. Those ancient 1980s were SO long ago.

Now the phenomenon of "content demand" from cable news has been multiplied exponentially by the website news phenomenon, with all the outlets seeking content, and the content being offered to viewers as "newsworthy." So the flow of information out of the government files has been given a remarkable amplification it had never experienced before. Expert analysis would precede government action on submitted data in the past; now the government acts as mere processor without judging the quality or significance of the reported data, leaving the analysis to the media and the public. This flow of government records, in turn, increased the stress on editors at the intake valve of reportable information, reducing their time available for analysis, verification, or for assuring the accuracy of what government was releasing or posting.

V. GOVERNMENT BECOMES A PROCESSOR

The Irish writer Flannery O'Connor wrote that "everything that rises must converge." Even outside that metaphor of theology, we find the new phenomenon of convergence of information and power. All the information flows from government websites that came into government from private regulated entities, government labs, and statistical and experimental sources are converging rapidly into what we may call "data-as-decisional-fuel." This rapid flow of fragments of information from many competing offerors of news content fuels the decisions we make as voters and investors and citizens. There is an information rivalry among content providers, print and broadcast, leading to the formation of a rough collective consensus about the optimally informed governance of the issues facing our modern American society. To the extent this trend calls in turn for greater amounts of data to flow freely, the government information machinery that once was a decisional *process* has become a mere *processor*.

An illustration of the "government as processor" role comes from part of the vast flow of federally-gathered environmental information. The Environmental Protection Agency's annual Toxic Release Inventory (TRI) statistics are expected to show on a year-to-year basis that chemical firms did or did not increase public risks. A rise in TRI numbers suggests more pollutants were being released; a local or particular facility increase will generate criticism and press releases that "spin" the statistical data. A fall in TRI numbers will be accompanied by proud media statements from the industrial community. But what is really happening may be quite different. The systemic flaws of the TRI system permit misperceptions of "rising pollution" as some facilities change, as the Environmental Protection Agency (EPA) changes the chemical list, as the scope of facilities covered changes, etcetera. Government is the processor and transmitter of the privately generated data. But the misperceptions about environmental performance expressed by competing media outlets are not the government's own criticisms—the government simply sets a reporting rule and then aggregates the private data for release to the public.

VI. REACTIONS TO THE NEW MODELS

The new models required reconsideration of the basic norm of total accessibility. Selective disclosure models were adopted in the 2002 Homeland Security Act and other developments forecast the end of a presumption that all requesters are equally benign in their desire to review governmental activities through information access.

A. Judicial Reactions

The motive of the information requester becomes a significant issue when the topical area of the request ventures into an area of FOIA disclosure that is governed by a mandate for balance. For example, the law enforcement informant has privacy interests under FOIA that are to be balanced against public needs,³⁴ when balancing is required, the requester's motives become a part of the equation.³⁵ One court denied a convicted terrorist bomber's request for FBI files because of a "high likelihood that Plaintiff's file contains information regarding previously less active 'sleeper cells' that the Government may need use to detect threats to the integrity of the nation's security."³⁶ Another court noted that the balancing of requester need and privacy concerns is affected by the requester-plaintiff's conviction for murder and his attempt at retaliation to murder a witness.³⁷ Judges are aware that the consequences of disclosure cannot always be foreseen, and this animates their consideration of the exemption claims relating to privacy interests.

B. Commercial Data Handling

Ever since the mid-1970s there have been disputes about whether private companies' submissions should be protected by the agencies, through the invocation of FOIA exemption 4 for trade secrets and confidential commercial information.³⁸ These disputes led to the Supreme Court's 1979 *Chrysler*³⁹ decision, which recognized the legitimacy of "reverse FOIA" suits, and to Executive Order 12,600,⁴⁰ which since 1987 has compelled Executive Branch agencies to give advance notice before they disregard a corporate submitter's claim of confidentiality for its commercial data.

One ironic twist of the post-September 11th era is that terrorist attacks have provided U.S. industrial entities that submit records to agencies with a receptive audience for their arguments favoring protection of such privately-submitted data. Prior to September 11th, skeptical agency decision makers and judges had downplayed industry claims of confidentiality in decisions and litigation about the consequences of disclosure. If the commercial data has a potential benefit to terrorists, then it may be withheld by agencies, the same agencies that had consistently refused to withhold upon the more mundane grounds of competitive injury.

Industrial operations often depend on the availability at the factory of sufficient storage to hold quantities of flammable or hazardous chemicals, such as the ink with which this paper has been printed. The manufacturing industry representatives have argued that they faced substantial costs. The advocates from Public Citizen, a public interest group, convinced a D.C. Circuit panel to abandon the 1938 Restatement of Torts norms of "trade secret" status⁴¹ to adopt the Canadian model instead, as a base

line for a more limited protection of business data.⁴²

C. Adverse Use Compared to Competitive Use

Before September 11th, the advocates of openness for infrastructure related data fought one opponent: commercial secrecy desires among the business community. The agencies' more frequent rejection of commercial entities' call for protections was the product of a drumbeat of advocacy organization complaints that agencies had given too much weight to the needs of industry.⁴³ After September 11th, the reality of "other" adverse use became quite evident. Our nation's adversary was a ruthless band of well financed, intelligent and disciplined terrorists, led by a man with a graduate civil engineering degree, Osama Bin Laden. The patterns of withholding may be changing but the nature of the data has not changed and the user's potential type of hostile use is the only variable that is different.

But the new focus on the user's intent runs directly contrary to the classic FOIA provision that "any person" gets access without regard to purpose or motive.⁴⁴ The ideal of generalized decisions meant that motives were only rarely discussed in the cases; the great majority of FBI and Drug Enforcement Agency requests came from prisoners whose motives were officially disregarded, just as requests from commercial competitors were officially disregarded. Of course, if the request was for documents on which the law required a balancing, this balancing test included the motives and utility of the records, e.g., such as for the retaliation killing of a witness by a convicted criminal's gang.

VII. EFFECTS OF THE SEPTEMBER 11th ATTACKS

The events of September 11th have met with several historically significant responses. First, the federal policy on FOIA disclosures was shifted in favor of withholding and away from comprehensive web-based disclosure. Second, the extent of web posting of releasable data was changed, in a belated attempt to reduce terrorists' access to data that could be used for another attack. Third, the cycle of specific exemption language was accelerated. FOIA exemption 3 allows Congress to create exclusions from FOIA by specifying them in other statutes.⁴⁵ This movement will insulate some new sets of data from public disclosure, making the so-called (b)(3) amendments more acceptable than ever before. I will address each of these in turn.

A. Federal Policy Shifts

The Bush Administration's directive that redirected the Executive Branch FOIA policies was accomplished through Attorney General John Ashcroft's Memoranda on FOIA of Oct. 12, 2001.⁴⁶ The policy tells agencies that are considering a possible claim of exemption to ask not whether disclosure would cause "foreseeable harm," a norm found in the Clinton Administration 1993 policy, but whether there is a "sound legal basis" in case law for withholding. The Justice Department promised to defend a claim of exempt status unless the claims "lack a sound legal basis or present an unwarranted risk of adverse impact on the ability of other agencies to protect other important records."⁴⁷ The choice to waive exempt status and disclose "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."⁴⁸

The 2001 policy calls for attention to privacy interests when making disclosure decisions. This is a factor that tends to favor enforcement agency withholding of case files and witness interview records. When the 2001 policy is compared to the former Clinton Administration's policy, the comparison makes for an interesting analysis: Clinton would avoid withholding, Bush will favor it; Clinton burdens those agencies who wish to withhold, Bush cautions those agencies who wish to release; Clinton made disclosure despite an available exemption into a norm of policy, while Bush made such waivers a cautiously evaluated exception.

Then a March 2002 directive by the President's Chief of Staff told federal executive agencies to: (1) place under the classified-documents status "information that could reasonably be expected to assist in the development or use of weapons of mass destruction" and (2) protect from inappropriate disclosure "sensitive" information about infrastructure, on a case-by-case basis, balancing the risk of terrorists' misuse of the data with the "benefits that result from the open and efficient exchange of scientific, technical, and like information."⁴⁹

B. Internet Postings Shrink

Removal of information from U.S. government websites has begun, but what is more significant is the decision not to post certain data that might be useful to the "axis of evil." Vulnerability of a U.S. system, such as banking or chemical production or airports, are likely to be exposed in the regulatory files of inspections, evaluations, plans, etcetera. Regulators track these vulnerabilities as part of their mission to protect the public. Web posting would in theory have aided that mission by encouraging public attention to cleanup of the deficient regulated entities. But after September 11th, posting a vulnerability was seen as an invitation to potential attackers.

For example, a CD-ROM describing the vulnerability of U.S. water supply dams was removed from circulation and destroyed by orders from the U.S. Geological Survey to federal depository libraries. The EPA is reconsidering the posting of information about risks from chemical facilities. Other agencies are hesitant to point the world to the weaknesses of U.S. institutions.

C. The Scenario-Disclosure Retreat

Even before September 11th, Congress acted to specifically remove from the Internet the EPA sets of data concerning neighborhood health risks from the “worst case” disaster scenarios that could occur at plants handling higher risk chemicals. Lawyers for owners of some (but not all) large factories or processing plants have already completed the EPA’s mandatory worst-case scenario reports as required by section 112(r) of the 1990 Clean Air Act.⁵⁰ A map of gas cloud dispersion, or “isopleth,” is plotted on top of a local map, showing which neighborhoods will be endangered by a chemical spill or release if all of the facility’s containment and protective measures failed to operate, in the worst case.⁵¹ The history of the section was that environmental lobbying organizations wanted to be able to challenge chemical producers, and they decided to use illustrations of the extreme cases of “off site consequences” as their best weapons. Now, the dissemination of data about remote risks might lose the perspective of “remoteness” as the general public hears smaller and smaller amounts of context with each news organization’s summarization of the news story.

One result of public dissemination about chemical hazards is wider public dissemination of what terrorists could do to accelerate the occurrence of risk scenarios. Internet posting has already carried worst-case scenario information⁵² about the local plants to civil engineers, such as the world’s most recognizable graduate civil engineer, Osama Bin Laden. The EPA, keeper of the mandatory submissions by chemical facilities, now has “the unenviable job of having to strike the difficult balance between the need for citizens to know about the facilities in their back yards and the need to protect those facilities from a terrorist threat.”⁵³

In 1990, as part of the massive Clean Air Act amendments, Congress imposed a requirement for certain plants to discuss their chemical release risks in terms of the “worst case” scenario in which all safeguards failed and total release to the atmosphere occurred.⁵⁴ The 1999 legislation amending 112(r) was a half-baked compromise—making the offsite consequence analysis public in ways that facilitate lessened dissemination, and spreading far and wide the other vulnerability data that has value to terrorists independent of the off-site consequences analysis maps. The 1999 amendment⁵⁵ limits the class of recipients to “covered persons” and makes it a crime to

disseminate the information beyond that class; if the owner of the data chooses to disseminate it to members of the public, then the owner must notify EPA that the document is now publicly available to that penalties do not apply.⁵⁶

The debate focused attention on the unintended consequences of Internet postings. If the owner of the facility kept the detailed data and maps confidential from the public, while sharing the data with federal and state officials, the special status of that data would merit extra protection in the form of a new federal crime: if the disclosure was made of a set of “restricted” data, willful violation of a disclosure restriction on such plans carries a fine of up to \$1,000,000 per organizational or individual discloser.⁵⁷

The 1999 legislation⁵⁸ modifying the risk management plan requirements in the 1990 Clean Air Act⁵⁹ also directed studies of the competing disclosure and secrecy interests; a subsequent Presidential Memorandum⁶⁰ required the FBI to “assess the increased risk of terrorist and other criminal activity associated with the posting of off-site consequence analysis information on the Internet” and ordered the EPA to “assess the incentives created by public disclosure of off-site consequence analysis information for reduction in the risk of accidental releases.”⁶¹ As this article was completed, the reports have not yet been made public.

D. Rise of FOIA-Proofing of New Statutes

A third phenomenon could be called “FOIA-proofing” new data requirements. There are approximately 150 specific clauses in federal laws whose language triggers the protection of specific sets of data from Freedom of Information Act disclosure. These clauses are of the types that can trigger the specific statutory exemption clause in subsection (b)(3) of the Freedom of Information Act.⁶² These so-called “(b)(3) laws” are the information equivalents of what the legislative drafters call “savings clauses.”

Notwithstanding the general FOIA and its normal pro-disclosure mandate, Congress could exclude a class of records from FOIA either by giving a mandate against *any* disclosure or by narrowly specifying the discretion of the agency to make a disclosure.⁶³ The Justice Department observed recently that most confidentiality laws enacted in the past had broadly precluded disclosure, but that a “growing trend” has increasingly arisen in which Congress “has been enacting legislation specifically focused on the prohibition of disclosure under FOIA only,” but “as yet no court has specifically discussed this more narrow legislative approach to nondisclosure.”⁶⁴

Most visible among these FOIA exemption triggers is the Internal Revenue Code’s prohibition against release of tax return data.⁶⁵ The risk management plan legislation discussed above also used FOIA specific-statutes exemption (b)(3) to

protect data submitted for an FBI security review of a chemical user facility; this data is exempt from FOIA if disclosure “would pose a threat to national security.”⁶⁶

Before September 11, the small Washington clique of FOIA advocacy insiders would scan any new legislation for the appearance of anti-disclosure terms that could trigger the (b)(3) provisions, and they would then argue against carving out public access to whatever the set of reports or documents would be. The world has changed since U.S. government documents were reportedly found in Al Qaeda possession in Afghanistan.⁶⁷ In 2002, a proposal was made to exempt certain business information under a (b)(3) exemption statute,⁶⁸ but this was cited as a “difficult issue” for negotiators over the 2002 Homeland Security Bill.⁶⁹ We can predict that there will be many more statutes adopted with FOIA exemptions triggered by the (b)(3) language written into the law, and some existing disclosure patterns will be changed by adoption of a new amendment to existing laws.⁷⁰

VIII. PREDICTIONS OF THE FUTURE

The rapid growth of access by the Internet-user “public” to federal documents, once on a vertically rising scale, will be moderated. If one can extrapolate from Homeland Security legislation, Congress will opt for lesser disclosure when vulnerabilities may be exposed. The future will be darker if another major terrorist attack occurs. This risk threatens the agencies’ perception of federal data users, a perception among many agencies and courts that overlooks the risks of the requester’s misuse.

A. What Operational Effects Will Be Seen?

The Internet postings of useful data from agency files are optional for federal agencies. Agencies are free to hold paper files and await requests—in the absence of a duty to publish rules⁷¹ or special legislation compelling them to post a particular subset of their information. The recourse for interested persons is to seek the same data from the agency under FOIA requests. The government-wide FOIA statistics continue to show increases in volume of requests. The 2,235,201 FOIA requests in fiscal year 2000 were up 13.5 percent from the preceding year despite the huge amount of data posted on the Internet. This is not a cost-free item; while there is no central cost figure for Internet posting of data, we know that the aggregate cost of FOIA processing in 2000 exceeded \$253 million, of which more than \$11 million was spent on FOIA litigation.⁷²

What if Internet posting of affirmative disclosures by agencies should decline, and requesters continue to send in FOIA requests? The ease and utility of requester-

initiated federal agency data searches will diminish, of course, and the cost of searches will go up. This assumes the nine FOIA exemptions remain as they were before September 11th. If FOIA world of available documents shrinks as a result of the 2001 Attorney General's Memorandum and the accompanying focus on secrecy, then fewer FOIA requests will be granted. Together with the Internet rescission or reduction in postings, this FOIA retrenchment may have a foreseeable impact on the transparency ideal. The effect may be to cumulatively constrain the general public's access to government files.

B. Will FOIA Be Changed?

Access to records by any person is a basic tenet of FOIA, but that may change. In addition to closing the outflow of FOIA pipeline by new exempt status decisions, the inflow of FOIA requests might be narrowed. The 2002 amendments to FOIA expressly forbid a federal intelligence agency such as the CIA or the Homeland Security Department's intelligence staff from answering FOIA requests made by a "representative" of a foreign "government entity."⁷³ With the exception of the intelligence and military functions, there does not seem to be a broad constituency for altering the "any person" access norm that applies generally across all FOIA operations.

FOIA procedures will probably not be altered by legislation, but if Congress were to alter it, the amendments would probably create a second tier of data; this would restrict the release of a limited class of data, narrowing access for selected recipients of sensitive data, while continuing FOIA norms for most agency records. This could be done by a selective waiver provision or a modification of FOIA's principle that "disclosure to one triggers disclosure to all." Whether or not this process is altered, the Congress will very likely continue to exclude sets of data from FOIA by confidentiality clauses in statutes that trigger the exemption 3 protection available under current FOIA.⁷⁴

Without amendments to FOIA, the current exemptions are premised on the 1960s vision of the classes of information users who were envisioned in 1963 to 1965 when the exemptions were created. These include the corporate targets of formal adjudications, the competitive makers of regulated products, and conventional criminals sought by police. In this decade, federal agencies that have a legitimate fear of misuse of infrastructure and commercial facility information by terrorists have several choices.

C. What Choices Do Agencies Have?

First, the agency could do nothing and hope none of its prodigious outflow of Web postings will fertilize the terrorists' plans with useful information. One will never know where the content of one's website has been used, until after the use has visibly occurred, and even then, an attribution to a particular FOIA request may be difficult.

Second, agencies could use existing commercial data exemptions more energetically to protect the individual private submissions relevant to infrastructure or homeland defense such as chemical antidotes for poisons or storage data on liquid propane sites. This possible mood favoring withholding under FOIA may take the form of more generous invocation of the *Critical Mass*⁷⁵ standard for voluntarily submitted data, under exemption 4 regarding trade secrets⁷⁶. The same motive would indicate that agencies deny exemption 4 status to submitted private data less frequently than they have tended to do in recent years.

Third, agencies could alter their FOIA regulations to better define classes of information that will not ordinarily be released. This builds upon Executive Order 12,600 and uses the agency's rulemaking that alters the current regulations as the forum in which to hear the expectations of the competing constituency groups.

Fourth, agencies could develop waiver programs similar to one undertaken by the Federal Energy Regulatory Commission. The disclosure of a special category of records under a procedure outside of normal FOIA channels⁷⁷ does not waive the exemption coverage for that category, unless the agency makes a decision to share the data.⁷⁸

Fifth, agencies could ask Congress to add exemption (3)-triggering clauses for particular sets of incoming submitted data to their next round of appropriations or enabling legislation. The flurry of such mini-exemptions could become a blizzard that would affect the ability of the public to monitor agency operations.

D. Concluding Questions

Empirical data will hopefully be available in the future when historians answer several important questions in retrospect. For now, I make my own predictions.

- Did the post-September 11th diminished access to government information cause a corresponding loss of the public benefits that could be derived from access? I predict that the public will indeed receive fewer benefits.
- Were perceptions about federal government operations more adverse to the agencies as a result of the diminished access? I predict yes, charges of concealment will affect credibility of some agencies, as military secrecy has caused suspicion of military announcements in the past.

Motives and Information Disclosure Laws

- Has this combination of anti-transparency forces (external threats from use of the released records) diminished the overall value of public access to government records? I think not yet, but trends could take it to that point.
- In terms of trends, did September 11, 2001 mark the end of the momentum toward a fully transparent government? For the near term, my answer is yes; for the long term, that depends on how long the present critical conflicts will continue.

The answers are intriguing and may affect our future relationships toward federal and state government. In the meantime, the evolution of information policies in the post September 11th world is well worth watching.

Notes

1. Although Sweden is said to have such rights from the 18th century, there were no models of such legislation when the U.S. law was being drafted in the early 1960s.
2. *KQED v. Houchins*, 438 U.S. § 1 (1978); *Ctr. for Nat'l Security Studies v U.S. Dept. of Justice*, 2002 Westlaw 1773067 (D.D.C. 2002) (appeal pending). *See also Wolfe v Froehlke*, 358 F.Supp. 1318, 1321 (D.D.C. 1973), *aff'd.*, 510 F.2d 654 (D.C. Cir., 1974), stating that there is no "affirmative duty on the part of the Government to assist in . . . research or to disclose Government files."
3. Pub. L. 89-554, 80 Stat. 383 (1966).
4. Military classification of the operational details prevents conventional source footnoting on this point, of course.
5. Kelli Arena and David Ensor, *U.S. infrastructure information found on al Qaeda computer*, at www.cnn.com/2002/US/06/27/alqaeda.cyber.threat.
6. This "compelled speech" would violate the First Amendment, and the "taking" of private data without consent might be compensable under the Fifth Amendment, in addition to the probable recognition of individual rights to privacy.
7. Government's ability to obtain the specific data under contract or under regulation seems to be a determining factor. *See, e.g., Shelby Amendment. But see Forsham v Harris*, 445 U.S. 169 (1980).
8. 5 U.S.C. §552(b)(1-9) (West 2002).
9. *Id.* at §552(a). There are some exceptions within the statute, however.
10. The extent of newspaper and broadcasting pressures to win approval of the changes, over persistent agency opposition, is summarized in 1 JAMES T. O'REILLY, *FEDERAL INFORMATION DISCLOSURE* §2:3 (3d Ed. 2000).
11. *Id.*, summarizing the hearings in § 2:3.
12. Pub. L. No. 404, § 3, Section 3 of Public Law 404, 79th Cong. 2d Sess., 50 Stat. 237 (1946).
13. Experienced Washington-based reporters had such networks of leak-prone bureaucrats that they cannot call them outsiders. They complained that they needed more and more records and that

- legislation would force the agencies which employed their confidential sources to be more overt about their disclosures.
14. O'REILLY, *supra* note 10, at § 2.3.
 15. See U.S. Department of Justice Office of Information & Privacy, Summary of Annual FOIA Reports for Fiscal Year 2000 (2002), *available at* <http://www.usdoj.gov/oip/foiapost/2002foiapost3.htm> [hereinafter Dept. of Justice Office]. The figure may approach \$300 million for fiscal 2001 when final statistics are compiled.
 16. N.Y. PUB. OFF. LAW § 89(3) (West 2003).
 17. VA. CODE ANN. § 2.2-3704(A) (West 2003).
 18. OHIO REV. CODE § 149.43(B)(4) (West 2002).
 19. CAL. GOV'T. CODE § 6252.5 (West 2003), stating that "an elected member or officer of any state or local agency is entitled to access to public records of that agency on the same basis as any other person."
 20. Ireland, Freedom of Information Act § 6-1, 1997, *available at* <http://www.bailii.org>.
 21. United Kingdom, Freedom of Information Act (2000), ch. 36 § 1(1), *available at* <http://www.legislation.hmso.gov.uk/acts/acts2000/00036--a.htm#1>.
 22. Ireland, Freedom of Information Act § 11, 1982, *available at* <http://www.ag.gov.au>, stating:
 - (1) Subject to this Act, every person has a legally enforceable right to obtain access in accordance with this Act to:
 - (a) a document of an agency, other than an exempt document; or
 - (b) an official document of a Minister, other than an exempt document.
 - (2) Subject to this Act, a person's right of access is not affected by:
 - (a) any reasons the person gives for seeking access; or
 - (b) the agency's or Minister's belief as to what are his or her reasons for seeking access.
 23. Commission of the European Communities, Proposal for a Directive of the European parliament and of the Council on public access to environmental information, 2000/0169 (COD), June 29, 2000, at 11, *available at* http://europa.eu.int/eur-lex/en/com/pdf/2000/en_500PC0402.pdf.
 24. Access to Information Act, R.S.C., ch. A-1, § 3 (1985) (Can.); Access to Information Act, R.S.C., ch. 21, § 4 (1992) (Can.).
 25. 5 U.S.C. § 552(b)(7) (West 2002).
 26. The legislative history and contemporaneous press coverage of FOIA shows virtually no business commentary to exemption (b)(4), but one business group obviously carved out its own protection in exemption (b)(9) for "oil and gas wells." 5 U.S.C. § 552(b)(9) (West 2002), *see* O'REILLY, *supra* note 10, at § 18.2.
 27. 5 U.S.C. § 552(a)(3) (West 2002) is passive; arguably the Federal Register disclosure provisions are more "active," 5 U.S.C. § 552(a)(1) (West 2002) but they are quasi-legislative directives and not the same character as information about which persons wish to inquire.
 28. See JAMES T. O'REILLY, UNIONS' RIGHTS TO COMPANY INFORMATION 234 (1987) (describing this incident and the response).
 29. DBCP, or dibromochloropropane, "is a potent carcinogen and perhaps the most powerful testicular toxin ever made. The pesticide causes genetic mutations and cancer in every species of animal on which it has been tested, in both sexes and by all routes of exposure -- ingestion, contact with the skin, and inhalation." Environmental Working Group Report, *Tap Water in 38 Central Calif.*

Motives and Information Disclosure Laws

- Cities Tainted With Banned Pesticide, available at*
<http://www.ewg.org/reports/dbcp/dbcpreport.html>.
30. Oil Chemical & Atomic Workers Union ALERT A-110 from A.F. Grospiron to All Local Union Presidents, *The Right to Know* (Oct. 11, 1977).
 31. *See* 29 C.F.R. § 1910.1200 (West 2002).
 32. *See* 42 U.S.C. § 11001 (West 2002).
 33. *See* 42 U.S.C. § 7412(r)(6)(K) (West 2002).
 34. *See* 5 U.S.C. § 552(b)(7)(C) (West 2002).
 35. *See* O'REILLY, *supra* note 28, at § 17:58, summarizing approximately 300 case decisions on this issue.
 36. *See* Ayyad v. U.S. Dept. of Justice, 2002 WL 654133, at *3 (S.D.N.Y. Apr. 18, 2002).
 37. *See* Shores v. Fed. Bureau of Investigation, 185 F.Supp.2d 77, 84 (D.D.C. 2002).
 38. 5 U.S.C. § 552(b)(4) (West 2002).
 39. *See generally*, Chrysler Corp. v. Brown, 441 U.S. 281 (1979).
 40. *See* Exec. Order No. 12,600, 52 Fed. Reg. 23,781 (June 23, 1987).
 41. RESTATEMENT OF TORTS § 757 cmt. b (1938).
 42. *See* Public Citizen Health Research Group v. Dept. of Health, Educ. & Welfare, 668 F.2d 537 (D.C. Cir., 1981).
 43. *See generally*, Public Citizen Health Research Group v Fed. Dept. of Agric., 704 F.2d 1280 (D.C. Cir., 1983) (advocacy group persuaded appeals court to abandon classic trade secrets test as applied to research data of medical device developers).
 44. *See* 5 U.S.C. § 552(a)(3) (West 2002).
 45. 55 U.S.C. § 552(b)(3) (West 2002).
 46. Memorandum from John Ashcroft, Attorney General, to Heads of all Federal Departments and Agencies (Oct. 12, 2001) *available at* www.usdoj.gov/oip/foiapost/2001foiapost19.htm.
 47. *Id.*
 48. *Id.*
 49. Memorandum from Andrew Card, Assistant to the President and Chief of Staff, to Heads of Agencies (March 19, 2002), at Attachment (citing Memo from Laura Kimberley, Richard Huff and Daniel Metcalfe, to Departments and Agencies, *available at* <http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm>).
 50. *See* 42 U.S.C. § 7412(r) (West 2002).
 51. 40 C.F.R. § 68.25 (2002).
 52. *Id.* This information was publicly available on the Internet before August 2000, when new legislation went into effect that constrained its dissemination. *See* Pub. L. 106-40, 113 Stat. 207 (1999).
 53. Stephen Gidiere and Jason Forrester, *Balancing Homeland Security and Freedom of Information*, 16 ABA NAT. RESOURCES & ENV'T. 139, 144 (2002).
 54. *See* 42 U.S.C. § 7412(r) (West 2002).
 55. *See id.* at § 7412(r)(7)(H).
 56. *Id.* at § 7412(r)(H)(III).
 57. 42 U.S.C. § 7412(r)(H)(v)(II) (West 2002).

58. See Pub. L. 106-40, 113 Stat. 207 (1999).
59. See 42 U.S.C. § 7412(r)(7)(H)(ii)(I)(bb) (West 2002).
60. Presidential Memorandum, 65 Fed. Reg. 8631 (Jan. 27, 2000).
61. *Id.*
62. 5 U.S.C. § 552(b)(3) (West 2002).
63. See *id.*
64. U.S. Dept. of Justice, Freedom of Information Act Guide & Privacy Act Overview 156-157 (2002).
65. See 26 U.S.C. § 6103 (West 2002)..
66. 42 U.S.C. § 7412(r)(7)(H)(xi)(III) (West 2002).
67. See Kelli Arena and David Ensor, *U.S. Infrastructure Information Found on Al Qaeda Computer*, (June 27, 2002), available at www.cnn.com/2002/US/06/27/alqaeda.cyber.threat.
68. See 5 U.S.C. § 552(b)(3) (West 2002) (providing an exemption from required disclosure that is triggered by a particular federal statute that mandates withholding or provides narrow disclosure criteria).
69. Associated Press, *Dems Dismiss Homeland Veto Threat* (Sept. 7, 2002), available at <http://www.cbsnews.com/stories/2002/09/03/september11/main520589.shtml>.
70. In addition, agencies may follow the lead of the Federal Energy Regulatory Commission and create a parallel route of preferred disclosures outside of FOIA channels. See Proposed Rules, 67 Fed. Reg. 57,994 (Sept. 13, 2002) (proposed rules amending 18 C.F.R. § 388.112).
71. See 5 U.S.C. § 552(a)(1) (West 2002).
72. See DEPARTMENT OF JUSTICE, *supra* note 15.
73. 5 U.S.C. § 552(a)(3)(E)(ii) (West 2002).
74. See 5 U.S.C. § 552(b)(3) (West 2002).
75. See *Critical Mass Energy Project v. Nuclear Regulator Commission*, 975 F.2d 871 (D.C. Cir. 1992) (construing FOIA).
76. 55 U.S.C. § 552(b)(4) (West 2002).
77. Most agencies regard all requests as FOIA requests, but the Federal Energy Regulatory Commission proposed rule creates a separate path for sensitive data requests by favored requesters. See Proposed Rules, 67 Fed. Reg. 57,994 (Sept. 13, 2002).
78. See *id.*