

Records and Information Management Perspectives

Part 2: Access to Public Information

by Lee S. Strickland

Editor's note: "Records and Information Management Perspectives, Part I: Legislative and Legal Developments," appeared in the June/July 2003 issue of the *Bulletin*.

Lee S. Strickland, J.D., is visiting professor in the College of Information Studies at the University of Maryland. He can be reached by e-mail at LSTRICKL@deans.umd.edu

Concerns have been present for some years that our laudable drive for "openness" has led to the inopportune disclosure of sensitive information affecting our national security. However, the renewed importance of homeland security in the face of threats from international terrorism have required that we diligently re-examine our policies on public access to government information – both in terms of voluntary releases, such as publication on government websites, and mandated disclosures under the Freedom of Information Act (FOIA) and numerous other disclosure statutes. *As a matter of policy, how should we balance our rights to government information as members of a democratic society when, at the same time, such information could benefit terrorists?*

Indeed, the issue of *openness* is even broader given the following permutations: First, consider the various holders of sensitive information – from corporations that fear providing information to the

government to private scientific publishers who value the importance of scientific information exchange but nevertheless acknowledge that certain information may present national security risks. Second, consider that we must address not only sensitive national security issues but individual privacy issues as well. As citizens, we generally applaud openness until we realize that our personal information may be threatened with disclosure. And third, consider the growing role of private information brokers for government information. *Does the insertion of private enterprise in the life-cycle of government information mean that citizens risk the integrity of critical information as well as their rights under existing law to require accuracy and amendment as necessary? In sum, the question presented: Where is national information access policy today – and tomorrow?*

Openness and National Security. Beginning more than five years ago, certain sectors of the Executive

branch and Congress began to fear that mandated FOIA releases were, in the aggregate, revealing information harmful to national security. This was perhaps most evident in the actions of former Department of Energy Secretary O’Leary in the Clinton administration and her push for openness that resulted in Congressional direction to review immense volumes of information that had been cleared for release. And it was more recently evident – also beginning several years ago but accelerating in the aftermath of September 11 – where many agencies have reconsidered information currently on the Web or otherwise available to the public. These changes in access ranged from documents impinging on intelligence sources and methods related to Gulf War Veterans’ Illness to worst-case scenarios prepared for the Federal Emergency Management Agency to mandated disclosures on community water treatment programs by the Environmental Protection Agency (EPA). By way of very specific examples, the EPA removed some 9,000 documents (including many scientific research papers that referenced “nuclear” or “chemical” or “storage”) as well as Envirofacts database that allowed people to search for information about environmental issues in their neighborhoods and received more than 100 million hits a month. The critical point is that each of these instances, and hundreds of others, presented a very real conundrum between the needed release of information of great import to Americans – and the feared benefit to our adversaries.

It was for such reasons that Attorney General (AG) Ashcroft on October 12, 2001, announced a reversal of the policy of former AG Reno who had urged discretionary releases unless it was “*reasonably foreseeable that disclosure would be harmful.*” Indeed, Ms. Reno had established a presumption of “*maximum responsible disclosure of information ... that 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.*” As she explained the issue, the “American public’s understanding of the workings of its government is a cornerstone of our democracy...[and]...we make government throughout the executive branch more open, more responsive and more accountable.”

The new policy allows governmental agencies to withhold whenever there is a legal basis to do so and is based, according to the Department of Justice, on “the importance of protecting sensitive institutional, commercial and personal interests that can be implicated in government records – such as the need to safeguard national security, to maintain law enforcement effectiveness, to respect confidentiality, to protect internal agency deliberations and to preserve personal privacy.” In other statements to highlight the deference that will be given

to individual agencies in their withholding decisions, Mr. Ashcroft has stated that “when you carefully consider FOIA requests and decide to withhold records, in whole or in part, you can be assured that the Department of Justice will defend your decisions unless they lack a sound legal basis or present an unwarranted risk of adverse impact on the ability of other agencies to protect other important records.”

Following this policy change, Andrew Card, Jr., the White House Chief of Staff, directed agencies on March 19, 2002, to reexamine how they protect information that could be used by terrorists and report the results of their efforts to the Office of Homeland Security within 90 days. Specifically the memo calls for the classification or reclassification of information on weapons of mass destruction, directs agencies to classify such information if it has never been classified, irrespective of age, provided that it has not been disclosed to the public under proper authority, and further directs reclassification of sensitive information concerning nuclear or radiological weapons if, although it had been declassified, it had never been disclosed under proper authority. The directive further suggests that “*sensitive but unclassified*” information could be protected under other FOIA exemptions including Exemption 2 for information about the “*critical infrastructure*” where disclosure of internal agency records might cause a risk that

Research and Further Information Guide

See www.ombwatch.org for detailed information on federal government information withdrawals. Also note that such security concerns have not been limited to the federal arena and have been major concerns in the states. Many legislative proposals were criticized because of the lack of standards for withholding. (For example, in Maryland, it was proposed that a government official could deny access to records relating to public security simply if the official “*determines that inspection of the information would constitute a risk to the public or to public safety.*”) And many openness advocates such as the Reporter’s Committee for Freedom of the Press have also noted that the “*public has incredibly strong interest in knowing what the government is doing to protect the public.*” In the end, most of these state proposals were generally rolled back to more reasonable levels with definitive reference to specific information to be protected. (For instance, Maryland SB 240 authorizes withholding of “specified response procedures or plans prepared to prevent or respond to emergency situations; specified building plans, blueprints, schematic drawings, diagrams, operational manuals, or records of other buildings or structures operated by the State or any of its political subdivisions; or specified records prepared to prevent or respond to emergency situations” provided and only to the extent that access would jeopardize the security of a structure, facilitate the planning of a terrorist attack, or endanger the life or physical safety of an individual.)

laws or regulations could be circumvented or Exemption 4 for information voluntarily provided to the government by the private sector.

The primary concern with all of these efforts to reduce openness is not that certain previously available government information may prove of value to terrorists – and perhaps should be protected – but that there are no standards for making the new determinations.

Most recently, federal legislative action on openness has been in the context of legislation to establish a Department of Homeland Security (DHS) with the House and the Senate taking significantly different approaches. Initially (in 2002), the House version of the Homeland Security Act (HSA) included a broad new FOIA exemption for information voluntarily submitted to the new department with somewhat vague definitions and also preempting all state open records laws. The Senate version included a fairly narrow FOIA exemption for documents submitted to the new department that concerned vulnerabilities and contained no preemption of state open records laws. However the change in the Senate resulting from the November 2002 elections resulted in passage of a final HSA that included the broad exemption for information supplied to the government. Section 204 of the act specifically encourages the sharing of information with the DHS by the private sector, state and local governments, and individuals. It does so by providing that information voluntarily provided by non-federal parties to the DHS that relates to infrastructure vulnerabilities or other vulnerabilities to terrorism is not subject to public disclosure under the FOIA even if such information is forwarded by DHS to other federal agencies.

Openness and Individual Privacy. While openness policy tends to focus on national security interests, there is also a significant contest between openness and individual privacy in various contexts: required disclosures under the FOIA (or state equivalents), growing access facilitated by expanding e-government services and the exploding access provided by private data aggregators and the concomitant loss of “*practical obscurity*.”

We will briefly consider these in turn. First, the frequent invocation of the FOIA by private companies for information on individual citizens speaks for itself – many citizens and most courts believe that even the fact of communication between an individual and a government agency bears an expectation of privacy.

Second, the benefit and curse of e-government is less visible. We appreciate easy access to real estate and court records until we realize that our easy access is the same for everyone. At the present time, the federal and state courts are struggling with the issue of whether and to what extent the paper files (available to all in the courthouse) should be available online.

And lastly, we must consider the multiple risks posed by private data aggregators – businesses that compile and sell government information in electronic form – that are largely unregulated and that present enormous privacy implications.

Research and Further Information Guide

See *Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989), a FOIA case where access was sought to criminal history records. The U.S. Supreme Court held, *inter alia*, that privacy interests can exist even though the information has been made available to the general public at some other place and point in time – thus establishing a “*practical obscurity*” standard.

Consider by way of example, www.rapsheets.com, a company that has begun selling national criminal background checks for a small fee based on their compilation of some 50 million criminal records in 36 states, as well as any number of other companies selling all sorts of public record information including bankruptcies, divorce data, civil lawsuits or property ownership. First, there is the direct potential for an invasion of privacy by eliminating the concept of “*practical obscurity*” – a term of art used to recognize that privacy interests may exist in isolated data generally unknown to the public. And second, there is the equally real threat that in a *de facto* manner the public record may be corrupted. Consider the implications if such companies become the *de facto* holder and supplier of public record information. While the official public record would continue to be available at various courthouses or state agencies, few would have (or avail themselves of) access since the primary vehicle of dissemination and access would become the electronic version held by the private data brokers. The question then presented: *What becomes of the rights granted to citizens by state and federal privacy laws (for example, right of access, correction and accounting for disclosures)?*

In Sum

Records and information management (RIM) is no longer an arcane world of primary interest to a few. Our information age has converted the issue to one of critical importance to every corporate manager and each citizen – as information has become a key business asset and is similarly valued by individuals in terms of personal privacy. While we as information professionals tend to think in terms of availability, authenticity and reliability as key objectives for our RIM efforts, we must also verbalize another – security from theft. This has been one of the many concerns to the Cobell court, it is a vital concern in e-government implementations and is becoming a central focus of business information managers as they become cognizant of the significant liability issues. We shall consider in future installments a number of the legal and policy issues at play in the protection both of corporate data and customer data held by business.