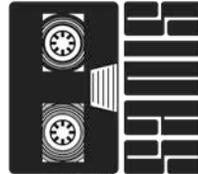


# B Sides

<http://ir.uiowa.edu/bsides>



U of I SLIS Journal

10|6|2010

## Freedom of Information Act and Libraries

Katherine A. Bullen

© copyright by Katherine A. Bullen, 2008

<http://ir.uiowa.edu/bsides/18>

*B Sides* is produced by Iowa Research Online, the University of Iowa's Institutional Repository

Katherine A. Bullen

Abstract

**Editors** | Katie DeVries Hassman & Julia Skinner  
**Layout & Identity design** | Colin Smalter

**Faculty Advisor** | Jim Elmborg

## Abstract:

The Freedom of Information Act (FOIA) makes government information accessible to everyone, including libraries and library patrons. The Patriot Act has undermined the FOIA and put the freedom to read at risk. This paper was previously presented in Cultural Foundations, Fall 2008.

### **Keywords:**

Freedom of Information Act | PATRIOT Act | Libraries

**B Sides** Fall 2010

<http://ir.uiowa.edu/bsides/18>



Kate Bullen  
021:101  
December 4, 2008

### **Freedom of Information Act and Libraries**

The Freedom of Information Act (FOIA) is an important piece of legislation for libraries. The acknowledged purpose of libraries is to make information available to the public at large, and the FOIA permits a greater scope of information to be available. The acknowledged purpose of FOIA is to make government information available to the people, including the government documents stored in repository libraries. The purpose of this paper is to provide an overview to librarians and others in the field of library and information science, of FOIA, the legislation leading up to this act, and the challenges to this act that also affect libraries.

#### **Historical Background**

President Lyndon Johnson signed FOIA into law on July 4, 1966. This act spelled out a right to know that is implicit in the First Amendment, and strongly advocated by the American Association of Newspaper Editors in the 1957 Declaration of Principles. In 1953, the Cross Report revealed that government documents were usually out of reach for the public, the press, and the courts alike, unless government officials *chose* to make said documents available (O'Brien, 1981).

Before 1966, there was the Administrative Procedure Act, the first, and not especially successful, attempt to make government documents available since the Housekeeping Statute of 1789. The Housekeeping Statute allowed each government department to create its own information dissemination policies. Many departments opted to release as little information as possible. The Administrative Procedure Act was a step forward, but a very small one. Requestors had to give a reason for wanting to see a given government document, and the request was often denied—"requiring secrecy in the public interest" or "required for good cause

to be held confidential”—even if the information was for the memoirs of a Confederate Army general, or a textbook on George Washington’s intelligence methods (O’Brien, 1981, p. 6).

### **Development of FOIA**

The FOIA was designed to eliminate personal discretion in the release of government documents. Everything is to be available for the asking, unless the information requested falls in one of the nine exemptions:

1. Under an Executive Order that the information be kept secret for national defense or foreign policy.
2. Part of the personnel rules or practices of a government agency.
3. Specifically exempted by law, provided that the law allows no room for interpreting otherwise than to withhold the work, or sets criteria for withholding the work which are satisfied.
4. Trade secrets and/or commercial or financial information.
5. Inter- or intra-agency memos/letters not available outside the agency—unless one is a direct party to a lawsuit with said agency.
6. Personnel or medical files.
7. Records compiled by law enforcement if releasing these records would a) interfere with law enforcement proceedings, b) deprive a person of the right to a fair trial, c) needlessly invade a person’s privacy, d) name a confidential source, e) disclose investigation or prosecution techniques, or f) endanger a person’s life or safety.
8. Records relating to financial institutions.
9. Geological information and maps regarding wells.

However, even if the records requested fall into one of these exemptions, the records may still be released if the exempted information is redacted before release (Henry, 2003, pp. 24-25).

FOIA has been amended several times. Following the Watergate incident in the Nixon White House, Congress strengthened the FOIA in 1975 (overriding a veto from President Ford)

by allowing judicial review of documents marked as classified, to ensure that they were properly classified. (Foerstel, 1999). In 1976, the FOIA was again amended as part of the Government in Sunshine Act. Congress also adjusted the request fee scale and the scope of access to national security and law enforcement records. In 1996, Congress passed the Electronic Freedom of Information Act Amendments. This E-FOIA confirmed that electronic documents are included in the scope of an FOIA request, and that agencies must also make more information available online, especially information that is not exempt under FOIA or information that is frequently requested (Foerstel, 1999, pp. 57-58). FOIA was amended again in 2002 in response to the terrorist attacks of September 11, 2001. This amendment limits the ability of foreign agents to request records from US intelligence agencies.

### **FOIA and the Patriot Act**

A significant problem arises when the government decides that freedom in information is a privilege rather than a right. Immediately following the terrorist attacks on September 11, 2001, Congress pushed through several pieces of legislation, the best known of which is the USA PATRIOT Act (Patriot Act). The Patriot Act has effectively rewritten several laws already in existence (Jaeger et al., 2004). The Foreign Intelligence Surveillance Act (FISA), for example, was originally written such that a wiretap may be obtained if “the purpose” was to obtain foreign intelligence. However, Section 218 of the Patriot Act amends this statement to read “a significant purpose” (Mart, 2004).

Section 215 has also expanded FISA statutes. The original law limited the types of businesses required to produce records or items for terrorism prevention investigations to car rental companies, storage rental companies, hotels and motels, and “common carriers” such as airlines, freight companies, and telephone or Internet providers. Now, however, “any business or

entity” (Mart, 2004) can be approached and asked to hand over any tangible item; this includes libraries and circulation records, Internet station sign-up sheets, even the golf pencils at the catalog stations, if necessary. Section 215 also has a built-in gag order, meaning that only the people who are required to retrieve the items in questions may know about the request. (Mart, 2004) The patrons can’t know, other library staff and administration can’t know, nor can the public know.

Section 216 allows for the use of pen registers. These devices originally recorded the digits dialed on a phone, thus allowing numbers called to be captured and used in criminal investigations. In 1972, the Supreme Court decided that no warrant was required to use a pen register, since the use of such a device was not a search as defined by the Fourth Amendment. In 1982, statute determined that pen registers could be used if the information retrieved was relevant to an ongoing criminal investigation. This referred only to capturing the digits dialed on a phone. However, the Patriot Act has reworded the law, so that computer routing or addressing information may be captured as well. Unlike telephones, where the number dialed and the content of the call require separate surveillance devices, computer routing and addressing information is applied to packets of information. These packets contain not only the IP address, the e-mail addresses of the sender and receiver, and the subject line; they also contain the body of the e-mail and/or the content of a Web site. Pen registers are only meant to capture non-content, phone number or IP address information (Mart, 2004). Content retrieval requires a warrant, which in turn requires probable cause: “a reasonable ground to suspect that a person has committed or is committing a crime or that a place contains specific items connected with a crime” (Garner, 1999). In addition, while other sections of the Patriot Act have a sunset

provision and will expire in time, section 216 does not. It will remain a law unless the Patriot Act is repealed (Mart, 2004).

### **Other Influences on FOIA**

The FOIA is strongly influenced by the Department of Justice and the Attorney General. It is customary for the Attorney General of a new Presidential Administration to issue policy statements regarding FOIA. (Uhl, 2004) Under Janet Reno, a “presumption of disclosure” was assumed regarding FOIA requests, and information that might technically be exempt was to be withheld only if it needed to be (Uhl, 2004). However, John Ashcroft reversed that policy: the requester must have a “need to know” the information. Such was government policy before the FOIA was created in 1966.

The government can make things difficult through its behavior as well. In 2007, FOIA requests were up almost 2 percent from 2006, but budgets and personnel were reduced by 3 percent and 8 percent, respectively. Very little progress has been made to handle backlogged requests at some agencies, and the number of requesters receiving all the information they asked for fell to a record low of 35.6 percent. (OpenTheGovernment.org, 2008).

The labeling of government information can also create problems. Classified information is, of course, classified and cannot be obtained. Some information needs protection and is not classified, such as personal privacy information or trade secrets, which are clearly exempted in FOIA itself. But other information, “Controlled Unclassified Information,” creates a problem. There is no standard labeling system; federal agencies can and do create their own labels, such as “For Official Use Only,” “Operations Security Protected Information,” and “Sensitive But Unclassified.” Even if several agencies have the same label, they may not apply the same standards in making that decision. The House of Representatives has passed two bills, the

Reducing Information Control Designations Act (H.R. 6576) and the Improving Public Access to Information Act of 2008 (H.R. 6193) (OpenTheGovernment.org, 2008). Both bills were received by the Senate, read twice, and referred to the Committee on Homeland Security and Government Affairs on July 31, 2008. No further action has been taken (THOMAS).

The government is a huge source of all sorts of information, from literacy statistics and unemployment rates, to rules for safely cooking and handling eggs. FOIA makes this information available, and libraries help raise awareness about the existence of this information. The Freedom of Information Act is a critical tool in allowing open access to information, for the libraries, as well as the public at large. This law has been challenged directly and indirectly, and only through vigilance and determined use can we ensure that it will remain on the books.

### **Additional Resources**

There are several places to find current information of the FOIA and related laws and policies. LexisNexis Congressional allows users to see the text of a bill, reports from committee and transcripts from hearings on the bill. However, this database requires a subscription and may not be available in all libraries. It is helpful, too, to know the name of the bill when searching for information on it.

The National Security Archive (<http://www.gwu.edu/~nsarchiv/index.html>) is a non-government library and research institute whose goal is to guarantee the public's right to know, and to make more of the historical record available, through FOIA requests and lawsuits. The National Security Archive has an extensive section on its Web site dedicated to the FOIA. The text of the law and its legislative development are there, as are links to recent legal developments and changes to the law, and instructions on how to file an FOIA claim. There is also the Digital

National Security Archive, a subscription-based database available through ProQuest (About the National Security Archive).

The Society of Professional Journalists FOI Committee is a volunteer network that looks for government attempts to limit public access to documents, as well as attacks against the First Amendment. While this organization consists of, and is directed to, journalists, the Web site is open to all, and the information on recent challenges to the FOIA is timely, with updates made about once a week.

### Bibliography

- Foerstel, H.N. (1999). *Freedom of information and the right to know: The Origins and applications of the freedom of information act*. Westport, CT: Greenwood.
- Garner, B.A. (Ed.). (1999). *Black's law dictionary (7<sup>th</sup> ed.)*. St. Paul, MN: West Group.
- Henry, C.L. (Ed.). (2003). *Freedom of information act*. New York: Novinka.
- H.R. 6193. (n.d.) In THOMAS. Retrieved November 23, 2008 from <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.06193>:
- H.R. 6576. (n.d.) In THOMAS. Retrieved November 23, 2008 from <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.06576>:
- Jaeger, P.T., McClure, C.R., Bertot, J.C., & Snead, J.T. (2004), The USA PATRIOT Act, the foreign intelligence surveillance act, and information policy research in libraries: Issues, impacts, and questions for libraries and researchers. *Library Quarterly*, 74, 99-121.
- Mart, S.N. Protecting the lady in Toledo: Post-USA PATRIOT act electronic surveillance at the library. (2004). *Law Library Journal*, 96, 449-474.
- O'Brien, D.M. (1981). *The Public's right to know: The Supreme court and the first amendment*. New York: Praeger.
- OpenTheGovernment.org. (2008). *Secrecy report card 2008: Indicators of secrecy in the federal government*. Retrieved November 23, 2008, from <http://openthegovernment.org/>
- Uhl, K. E. (2003). The Freedom of information act post-9/11: Balancing the public's right to know, critical infrastructure protection, and homeland security. *American University Law Review*, 53, 261-312.