

City University of New York (CUNY)

CUNY Academic Works

Publications and Research

CUNY School of Law

2013

Why Library Cards Offer More Privacy Rights than Proof of Citizenship: Librarian Ethics and Freedom of Information Act Requestor Policies

Sarah Lamdan
CUNY School of Law

[How does access to this work benefit you? Let us know!](#)

More information about this work at: https://academicworks.cuny.edu/cl_pubs/20

Discover additional works at: <https://academicworks.cuny.edu>

This work is made publicly available by the City University of New York (CUNY).
Contact: AcademicWorks@cuny.edu



Why library cards offer more privacy rights than proof of citizenship: Librarian ethics and Freedom of Information Act requestor policies

Sarah Shik Lamdan*

CUNY School of Law, 2 Court Square, Long Island City, NY 11101, USA

ARTICLE INFO

Available online 19 February 2013

Keywords:

FOIA
Librarians
Privacy
Ethics
Data

ABSTRACT

This paper demonstrates the divergent requestor privacy policies of professional librarians and the administration of the Freedom of Information Act (FOIA), and urges the federal government to adhere to librarian ethics in order to protect FOIA requestors. Section 1 of the paper provides information about the origins and purpose of the FOIA. Section 2 offers an overview of the philosophical and historical origins of library patron privacy ethics, discussing both the ethical basis for patron privacy and actual instances where library records have been sought for government surveillance of private citizens. Section 3 describes the state library laws that protect library requestors, as well as federal laws that protect non-FOIA requestor privacy rights, including the Video Privacy Protection Act (VPPA), which protects video rental records. Section 4 of the paper warns that, in the digital era, it is more important than ever to safeguard personal information like that contained in FOIA requests to prevent the stifling of information seeking activities in the United States. By modifying laws to meet the needs of the “information age,” the United States government can embrace and utilize the ethical standards that are at the foundation of librarianship, and protect the principle that information should be free and available to the American populace.

© 2013 Elsevier Inc. All rights reserved.

1. Introduction

On May 1, 2012, the American Library Association's (ALA) “Choose Privacy Week” celebrated information privacy with library events around the nation. The ALA's goals for the week included educating people about their personal privacy rights and informing the public about eroding privacy standards in the internet world. The website announcing the week's events warns that “Citizens turn a blind eye to the fact that online searches create traceable records that make them vulnerable to questions by the FBI, or that government agencies can track their phone calls, airline travel, online purchases, and more.” (American Library Association Office for Information Technology Policy, 2012).

This librarian salute to privacy rights raises a question: Why are libraries and librarians shouldering the responsibility of warning the public about privacy invasion? After all, isn't this a task better suited for police enforcement, consumer protection groups, or state and federal governments?

As it turns out, librarians, more than many other professional groups, engage in pro-privacy practices. They have developed high privacy standards for people seeking information. As explained by the ALA, “Librarians feel a professional responsibility to protect the right to search

for information free from surveillance.” (American Library Association Office for Information Technology Policy, 2012). Patron privacy is a cornerstone of library services in America.

In contrast to American librarians, American government officials sometimes put private citizens' privacy rights in peril. In the halls of Congress, state representatives take actions that threaten the privacy of those searching for government information.

One example of government disregard for personal privacy comes from California Congressman Darrell Issa. In 2011, his call for the publication of a huge catalog of Freedom of Information Act of 1966 (a law commonly called the FOIA, located in the Administrative Procedure Act, which governs the activities of federal agencies) records raised the eyebrows of privacy advocates across the nation. Issa demanded that 180 federal agencies release data naming people who placed FOIA requests, the dates of their requests, and the information sought in those requests (Lipton, 2011). The congressman claimed that the logs would be used to reveal agencies' responsiveness to FOIA requests (Letter from Darrell E. Issa, Chairman, House Committee on Oversight and Government Reform, to FOIA Officers, 2011). Critics found the log request unduly invasive, because the logs contain information about members of the general public and their inquiries into government information and activities.

The intrusive nature of Issa's request drew criticism from personal privacy advocates. David Cuillier, a University of Arizona journalism professor and chairman of the Freedom of Information Committee at the Society of Professional Journalists called Issa's request, “An easy way to target people who [Issa] might think are up to no good”, and John

* Fax: +1 718 340 4276.

E-mail address: Sarah.lamdan@mail.law.cuny.edu.

Verdi, senior counsel at the Electronic Privacy Information Center worried that the requester information “could be used to track who the biggest gadfly is.” (Lipton, 2011).

Although Issa's FOIA log request raises ethical concerns, there are no laws to address the privacy of government information seekers' queries. There are no rules or standards to protect the people and entities that make FOIA requests. Contrarily, the FOIA is singularly focused on information transparency, to the detriment of FOIA requestors.

This lapse in protection becomes more important as the information digitization allows the government to maintain large electronic databases capturing personal information and electronic records track personal data. The National Institute of Standards Technology reports that the government collects private citizens' Social Security numbers, birth information, mother's maiden names, biometric records, and medical, educational, financial and employment information. This “can include telephone numbers, IP or Media Access Control addresses, or any static identifier that links to a single person or to a small, well-defined group of people.” (Jackson, 2010). In the internet age, personal information is easily disseminated and captured by the federal government. For example, the Library of Congress now archives every public Twitter tweet since Twitter's inception in March, 2006 (Raymond, 2010). This gives the government easy access to everything any citizen has ever typed on Twitter.

Some claim that government information can only harm you if you “have something to hide.” (Solove, 2011). Daniel J. Solove, professor of law at George Washington University warns, conversely, that government releases of private information can harm anybody, regardless of the person's criminal tendencies or status. Solove (2011) adds that, in the modern internet era, where the government has “large dossiers of everyone's activities, interests, reading habits, finances and health,” the government can piece together its own “story” about you and make determinations about you based on patterns of behavior.

The government's “dossiers” of personal information could easily include the questions that private citizens ask of the federal government through FOIA requests. FOIA requests and their associated materials could be pieced into your “personal story” and used to incriminate or define you. This chain of privacy-invasion logic is precisely the rationale behind librarians' privacy standards for library patrons.

Librarians, like government agencies' FOIA offices, receive information requests on a daily basis. However, unlike the federal government, the institution of librarianship has a code of ethics to protect requestors. From library school and throughout their careers, library professionals are trained to maintaining library patron confidentiality. Librarians take special care to protect their patrons' origins and identities and craft policies to swiftly discard patron information. As one librarian summarizes, “Collecting personal identity information about customers is a dangerous activity for a library. We should be careful to engage in it only when absolutely necessary.” (Ostrowsky, 2005).

Librarians' privacy standards are based in legally founded right to privacy. Warren and Brandeis (1890), in their benchmark paper identifying the tort of privacy invasion, compare privacy rights, specifically “the protection afforded to thoughts, sentiments, and emotions”, to “the right not to be assaulted or beaten, the right not to be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed”. According to Warren and Brandeis (1890), rights to privacy are guaranteed by the nation's common law, and a person cannot be forced to reveal his thoughts outside of a courtroom's witness stand.

Legal privacy for information requestors is recognized by state legislation protecting library patrons. States have enacted laws that explicitly protect library records from government surveillance and public exposure and some even protect State freedom of information requests in contrast to the lack of federal legislation.

Protecting information requestors, whether at library desks or government agency offices, is imperative to privacy rights in the United States (Peltz, Joi, & Andrews, 2006). Peltz et al. (2006), “Asking requestors to identify themselves and their motives results in a chilling

effect on access to public records. Chilling the anonymous exercise of rights is repugnant to classical ideas about individual rights.”

The value placed on requestor privacy by the library profession should also be applied to the government, in order to protect FOIA requestors with the same standards that are granted to library patrons. The federal government should adopt librarian ethics via federal statute like the Administrative Procedure Act, the FOIA, or a separate requestor protection law, to protect citizens' rights to seek information and “know what the government is up to.” (Department of Justice v. Reporters Commission For Freedom of Press, 1989, p. 777). This excerpt quotes Justice Douglas's dissent in Environmental Protection Agency v. Mink, 410 U.S. 73, 105 (1973), in which Douglas quotes from The New York Review of Books (Oct. 5, 1972, p. 7).

Section 2 of this paper offers a brief overview of the FOIA. Section 3 investigates the philosophical and historical origins of librarian patron privacy standards, and Section 4 demonstrates how those patron privacy standards have been successfully integrated into state law through library laws and the Video Privacy Protection Act on the federal level. Section 5 identifies a lack of patron privacy in the federal government's FOIA laws and demonstrates the dangers of denying privacy to FOIA requestors, who are, in essence, the patrons of the federal government's “library” of information. Finally, the paper concludes by urging the federal government to meet librarians' ethical rules for patron privacy.

2. A history of the FOIA

The FOIA was enacted by President Lyndon B. Johnson on July 4, 1966 as an amendment to the Administrative Procedure Act (Presidential statement on signing S. 1160, the Freedom of Information Act of 1966, 1966). The Administrative Procedure Act determines the processes governing federal agencies, including the required releases of agency information to the public. A more complete overview of the FOIA's history is addressed in Lamdan (2012). The FOIA was a reaction to reverse fears of government secrecy that pervaded the Watergate era (Finkelman, 2006). The prior version of the law was said to allow federal agencies to hide information from the public. It was derided as “an excuse for secrecy,” (United States, Senate Report 89-813) and called a “withholding statute” rather than a disclosure statute (United States. Congress. Senate. Committee on the Judiciary, 1965, p. 40). FOIA's passage into law was hailed as a beacon of government transparency and sunshine on agency information, which was previously shrouded in secrecy.

The most groundbreaking provision of the new FOIA allowed people to make requests for information not openly available to the public. Subsection (a)(3) created the ability to request information from federal agencies (United States Department of Justice, 2009, pp. 2–3). With some exceptions, people can ask for any information created or collected by federal agencies. Nine exemptions to this disclosure are built into Subsection (b) of the statute. These exemptions cover information that may be important to national security, or internal personnel and other internal matters, confidential business information, and personal information about private individuals (The Freedom of Information Act of 1966, 2010).

The FOIA has remained a highly relevant and frequently used federal law, and Congress has made sure that the FOIA's transparency standards modernized with the internet age and more frequent use of technology as an information collection tool. In 1996, President Bill Clinton signed the Electronic Freedom of Information Act Amendments into law to assure that FOIA would remain powerful and useful with rise of computer and internet use (Presidential statement on signing the Electronic Freedom of Information Act amendments 1996, 1996). This new legislation clarified that FOIA applies to records maintained in electronic formats, and “broadens public access to government information by placing more material online and expanding the role of the agency reading room.” (Presidential statement on signing the Electronic Freedom of Information Act amendments 1996, 1996).

3. Origins of library patron privacy ethics

Library privacy ethics have been driven by philosophical beliefs about privacy as a human right, the unique human trait of information-seeking behavior, and historical events threatening library patrons' liberties. These philosophies, human qualities, and historical happenings highlight the importance of privacy for all information seekers.

3.1. Philosophical origins of library patron privacy ethics

Library privacy policies are based upon the philosophical belief that both privacy and the ability to obtain information are basic human rights. This ethical determination comes from philosophical ideas, common law concepts, and constitutional premises regarding peoples' rights to access information privately. Philosophically, human privacy is associated with self-determination, dignity, and control. Michigan Supreme Court Justice, Thomas Cooley, put the importance of privacy above penal law concerns when he wrote, "it is better oftentimes that a crime should go unpunished than that the citizen should be liable to have his premises invaded, his trunks broken open, his private books, papers, and letters exposed to prying curiosity." (Cooley, 1868). Edward Bloustein, President of Rutgers University, said at a faculty and alumni symposium that privacy "defines man's essence as a unique and self-determining human being." (Bloustein, 1968). Privacy is seen as a basic human need, and the heart of personal identity. "Respecting the rights persons have to privacy is as basic a requirement as there can be in ethics." (Garoojian, 1991, p. 221).

This philosophical concept of privacy as a right has also taken hold in America's legal landscape. In their famous law review article, *Warren and Brandeis (1890)* find the basis for the right to privacy in common law, observing that, outside of the witness stand, Americans cannot be compelled to express their thoughts, sentiments, or emotions. The legal scholars extend the right to privacy liberally across all mediums of expression. They write,

"Neither does the existence of the right depend upon the nature or value of the thought or emotion, nor upon the excellence of the means of expression. The same protection is accorded to a casual letter or an entry in a diary and to the most valuable poem or essay, to a botch or daub and to a masterpiece. In every such case the individual is entitled to decide whether that which is his shall be given to the public." (Warren & Brandeis, 1890).

Warren and Brandeis use a phrase coined by Judge Thomas Cooley, "the right to be let alone" (Cooley, 1880), to summarize Americans' right to privacy. The authors expand this right beyond common law ideas to less ambiguous property right theories. Comparing daily private acts to copyrightable works, they analogize that even a note or diary entry, if deemed a literary composition, could be protected from copy by copyright (Warren & Brandeis, 1890). *Warren and Brandeis (1890)* also describe cases where courts have spared items that invaded personal privacy from publication using use property law or alleged breach of implied contract as grounds for protection. In the decisions, courts found in favor of protecting unpublished lectures (*Abernethy v. Hutchinson, 1825*), a catalog describing the Prince's etchings (*Prince Albert v. Strange, 1849*) and photographs of people (*Pollard v. Photographic Co., 1888*). In all instances, the idea is that one should not be compelled to reveal things close to oneself, like personal thoughts, physical bodies, and private acts.

Supreme Court justices have directly assigned constitutional protection to privacy. In *Griswold v. Connecticut (1965)*, a landmark privacy case dealing with the right to use contraception in marital relationships, Justice Douglas listed "the right to read" and "freedom of inquiry" as freedoms falling under First Amendment protection (*Griswold v. Connecticut, 1965, p. 482*). Additionally, *Stanley v.*

Georgia (1969), a case in which the Supreme Court reaffirmed a citizen's right to view pornography in the privacy of his own home, the court stated, "the Constitution protects the right to receive information and ideas." (*Stanley v. Georgia, 1969, p. 564*). Privacy rights are also inherent in the Fourth Amendment's protection from "unreasonable searches and seizures", and the Fifth and Fourteenth Amendments' exemptions to individuals from having to testify against themselves (*National Archives & Records Administration v. Favish, 2004, p. 221*).

Although the Supreme Court has directly identified privacy rights and defined particular aspects of privacy law, developing a legal landscape for privacy rights based in constitutional law theories, the court has not specifically addressed the privacy of information requesters. The Federal legislature has yet to address any facet of privacy concerns for those requesting information.

3.2. Historical origins of library patron privacy ethics

Library patron privacy rules and standards are not merely a result of philosophical pondering. Requestor privacy laws are enacted in reaction to historical events that make evident the need for such privacy measures. The American Library Association's (ALA) official policy of requestor confidentiality developed in reaction to attempts by the government to access library records to track and incriminate library patrons. In the 1960s and 1970s a confluence of government encroachment on library patron privacy forced the ALA to action. First, the Federal Bureau of Investigation (FBI) monitored seven-Vietnam War protesters' use of a college library to build a case against them. According to the FBI, the "Harrisburg Seven" conspired to kidnap Henry Kissinger, blow up generators in heating tunnels in Washington D.C., and vandalize draft board offices. The FBI intended to use library surveillance and librarian informants as evidence of their characters and intentions (Kennedy, 1989).

Around the same time, Federal Treasury agents demanded that public libraries across the country release circulation records recording the names and identifying information of people who checked out books on bomb making (Kennedy, 1989, p. 742). When this occurred, the American Library Association decried the Treasury's investigations as an unconscionable and unconstitutional invasion of library patrons' privacy. In reaction, librarians conducted sit-ins and protests, which eventually prompted the ALA and IRS to negotiate guidelines on government access to circulation records (Kennedy, 1989, p. 743). The guidelines between the government agency and the librarian group were never finalized, however. In 1971, the ALA took an official stance on requestor privacy, drafting a *Policy on the Confidentiality of Library Records* (Kennedy, 1989). This policy declared that all "circulation records and other records identifying the names of library users with specific materials" must be held as confidential.

This spirit of patron protection in libraries remained strong long after the Harrisburg Seven and the bomb making inquiry. In 1975, an ALA Statement on Professional Ethics specified that librarians were to "protect the essential confidential relationship which exists between a library user and a library", and the ALA's 1980 Code of Ethics insisted that librarians must, "protect each user's right to privacy with respect to information sought or received, and materials consulted, borrowed, or acquired." (Kennedy, 1989, p. 744).

Librarians were again reminded of the need for patron protection in the 1980s when the FBI instituted its Library Awareness Program (Matz, 2008, p. 72). The operational name for the Library Awareness Program within the FBI was "The Development of Counterintelligence Among Librarians," a name implicating librarians as partners in surveillance. The Library Awareness Program was an FBI counterintelligence initiative that profiled Russian or Slavic-sounding last names as belonging to people who may be potential threats to national security, and then traced the reading habits of patrons with those names. If their reading interests were deemed suspicious (if their

reading interests included National Technical Information Service reports, for example), the FBI sought to monitor those patrons. The ALA's Intellectual Freedom Committee drafted an advisory statement to warn libraries of the impending privacy infringements and tell them how to avoid breaking their ethical obligations if faced with FBI surveillance, as well as a statement to the director of the FBI voicing their concerns about the agency's library program ([American Library Association Office For Intellectual Freedom, 2005](#)).

In 2000, librarians stood up to law enforcement with bookstores to protect requestor privacy when the Tattered Cover bookstore in Denver, Colorado was served with a search warrant for book purchase records sought for an investigation into a methamphetamine lab. Librarians spoke out in support of patron privacy, and the Supreme Court of Colorado ruled that federal and state constitutions do not allow law enforcement from discovering personal information about book purchases unless law enforcement can show the information is critical to prosecution ([Tattered Cover, Inc. v. City of Thornton, 2002](#)). The court held that, "Everyone must be permitted to discover and consider the full range of expression and ideas available in our "market-place of ideas", without fear of government surveillance or reprisal." ([Tattered Cover, Inc. v. City of Thornton, 2002, pp. 1051–1052](#)).

Today's ALA Code of Ethics maintains librarians' dedication to patron privacy. Noting that libraries and their employees have a "special obligation to ensure the free flow of information and ideas to present and future generations", the third ethical guideline upholds a privacy standard. It states, "We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted." ([American Library Association Office for Information Technology Policy, 2012](#)). Notice, the provision has been updated to cover information transmitted over the internet or other electronic mediums.

Librarians take extra steps to insure that their privacy policies stay current. They constantly update patron privacy procedures to account for the presence of modern technology in libraries. The ALA, in their, *Role of Librarians in Protecting Patron Privacy* (2012) webpage, urge library staff training and a "multi-pronged approach" to actively educating users about privacy when using the internet. Libraries also proactively protect library users from privacy pitfalls by adjusting technology settings to not save internet search and browsing histories, and librarians erase their own electronic circulation records after time periods so that the reading habits of users cannot be tracked ([Coyle, 2002, p. 55](#)). The Library Journal advises, in the Coyle article, that librarians "Keep the minimum information" to meet [] legitimate goals, and don't collect information 'just in case', as well as, "Keep the information only as long as you must," to avoid harboring patron information that could be retrieved by non-library entities.

Additionally, librarians challenge legislation that challenges patrons' rights to privacy. Librarians responded strongly to the passage of the USA PATRIOT Act with national activism and lobbying ([Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, 2001](#)). Librarians feared the USA PATRIOT Act, which allows warrantless searches of library patron records without specificity or probable cause in situations where terrorism is a "significant purpose" of the search ([Regan, 2004](#)).

Attorney General John Ashcroft mocked librarians for their concerns about the PATRIOT Act. He joked that, "the FBI is not fighting terrorism. Instead, agents are checking how far you have gotten on the latest Tom Clancy novel." Librarians, not finding humor in Ashcroft's quip, reacted to bring light to their privacy concerns, and the American Library Association (ALA) issued an official press release following Ashcroft's speech ([Coolidge, 2005, p. 18](#)).

The release explained librarians' concerns over the PATRIOT Act', discussing the privacy dangers involved with Section 215 and Section 505, which permits the FBI to obtain library records without judicial oversight. Since the PATRIOT Act was enacted, librarians have pushed for amendments to the Act, including the Freedom to Read Protection

Act, which would increase judicial and congressional oversight of Section 215 activity and require that a subpoena be subject to traditional judicial scrutiny when used to access library and bookstore records ([Zalusky, 2011](#)).

In 2003, when the Justice Department marked libraries as a logical target of surveillance, the ALA concluded, "librarians have a history with law enforcement dating back to the McCarthy era that gives us pause. For decades, and as late as the 1980s, the FBI's Library Awareness Program sought information on the reading habits of people from "hostile foreign countries," as well as U.S. citizens who held unpopular political views." ([Regan, 2004](#)).

Librarians operate on the motto *information wants to be free*, embracing the ideal that all information be accessible to all people. However, librarians view the freedom to access patron information as inconsistent with the freedom of information. In fact, librarians feel that revealing information about library visitors creates an environment in which potential patrons shy away from accessing information for fear that their private requests will be revealed to all. As one librarian writes, "In all cases, whether it be a request from a family member, a law enforcement agent, or a reporter, the librarian is ethically and legally bound to make every effort to protect the individual's right to privacy no matter how convincing the argument for the release of such information appears in the light of the greater good. The individual's right to privacy should take precedence over the rights of society." ([Kennedy, 1989, p. 793](#)).

4. Librarian patron privacy ethics in the law

Library privacy measures have been officially codified in state laws. Additionally, despite the FOIA's silence on privacy for information requestors in the federal government's "library" of information, federal laws have also been enacted under the premise of information-seeking privacy. For example the Video Privacy Protection Act of 1988 (VPPA) protects the video rental information of video store patrons with similar ethical goals as those achieved in the library setting.

4.1. State laws

States address privacy rights for library patrons through legislation. By enacting library privacy laws, they have given a legal structure to the concept of patron privacy. These legal structures can serve as models for FOIA patron privacy measures that would legally guarantee the privacy of FOIA requestors.

State library patron privacy laws appeared in the late 1970s, as the aftermath of the Watergate scandal and the increasing use of computers to store personal data drew the public's attention towards personal privacy issues. Legislative action became a tool for securing the privacy ethics dictated by librarians' professional rules. Law Librarian [Bruce Johnson \(1989, p. 796\)](#) writes that, "With few exceptions, the legal protection of the privacy of library circulation records in this country has been statutory." States affirmatively create laws protecting library patron requests, aligning official state standards with library ethics.

Florida led the states in enacting legislation in 1978 ([Johnson, 1989, p. 796](#)). The Florida law makes public library records confidential and exempt from information inquiries. The Florida law makes registration and circulation records confidential, specifying that "no person" can make known "in any manner" the information within library requestor records except in following a "proper judicial order." ([Fla. Stat. § 257.261, 2011](#)). Breaking the library requestor privacy law is a misdemeanor.

Many states followed Florida's lead, drafting library patron privacy measures. Some states' laws make exceptions for disclosing information about minor children to their parents, notifying patron of overdue fines or missing books, and routine duties of library clerks, but the right of privacy against the general public for library records

is maintained on a state level (e.g., Ala. Code § 41-8-10, 2011; Ark. Code Ann. § 13-2-701, 2011a; Colorado Revised Statutes § 24-72-204(3) (2011); La. Rev. Stat. Ann. § 44:13, 2011).

Arkansas passed a law that goes as far as to require library record-keeping systems to maintain patron anonymity. In Arkansas, “Public libraries shall use an automated or Gaylord-type circulation system that does not identify a patron with circulated materials after materials are returned.” (Ark. Code Ann. § 13-2-703(b), 2011b). New Mexico directly associates its patron requestor rights with values imbedded in the state’s constitution: “The purpose of the Library Privacy Act is to preserve the intellectual freedom guaranteed by... the constitution of New Mexico by providing privacy for users of the public libraries of the state with respect to the library materials that they wish to use.” (N.M. Stat. Ann. § 18-9-2, 2010).

As of 2008, forty-eights states adopted library patron confidentiality laws (Matz, 2008, p. 76). The protections range from library-specific statutes to FOI request exemptions for library patron information. Hawaii and Kentucky, the only two states lacking such legislation, have “reliable AG opinions that identify library records as different from other state government files and therefore not in jeopardy of being disclosed under open record laws.” (Matz, 2008, p. 76). The Kentucky opinion, written by Attorney General Steven L. Beshear in 1981, says, in part, “We think that the individual’s privacy right as to what he borrows from a public library (books, motion picture film, periodicals and any other matter) is overwhelming.” Beshear summarizes, “We believe that the privacy rights which are inherent in a democratic society should constrain all libraries to keep their circulation lists confidential.” (Public Inspection of Public Library Records, Op. Att’y Gen 82–149, 1982).

Wisconsin and Minnesota have extended librarian privacy theories to their FOI request records (Citizen Advocacy Center, 2008). Wisconsin statute declares that, “no [FOI] request... may be refused because the person making the request is unwilling to be identified or to state the purpose of the request.” (Wis. Stat. § 19.35(1)(a)(i), 2008). Minnesota’s Government Data Practices Act also explicitly protects individual’s anonymity in making public records requests. “The law specifically states that a requestor need not identify himself or herself. In addition, no explanation for why public data is being requested is necessary, except for the sole purpose of facilitating data access.” These provisions incentivize those who “are concerned about government retaliation” to continue to use the law in the same way that librarian privacy incentivizes information seeking.

4.2. Federal laws: the Video Privacy Protection Act (VPPA) and beyond

Like state laws, some federal laws protect information seekers. The VPPA is an excellent example of federal government acting to protect the privacy of requestors. The VPPA was drafted after a Washington newspaper obtained and published a list of Robert Bork’s family’s video rentals during confirmation hearings for his nomination to the Supreme Court. The VPPA of 1998 prevents the wrongful disclosure of video rental and sale records. If a video provider discloses patrons’ rental information, they are liable for up to \$2500 in actual damages. Several class action lawsuits have come from this legislation, including a case against Blockbuster for allowing their online customers’ video rental selections to involuntarily appear on their Facebook pages (Harris v. Blockbuster, 2008). Lawsuits were also brought against Netflix in 2011, for holding consumer information longer than necessary (Milans v. Netflix, Inc., 2011; Sevy v. Netflix, Inc., 2011). The VPPA requires rental companies to “destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected.”

The protection of citizens’ video rental requests by the federal government is evidence of a government concern for requestor privacy. Although the federal government does not explicitly acknowledge or

uphold a librarian’s standard of ethics, the VPPA indicates that American law regards information seeking as a private activity.

Other federal laws also indicate the same concern for safeguarding personally identifiable information and records similar to the types of information found in FOIA requests. Laws bind state and federal agencies from releasing certain types of information about private citizens. For instance, the Computer Matching and Privacy Protection Act prohibits government agencies from using personally identifiable data for purposes other than those prompting the data’s collection (Relyea, 2001, p. 42). The Driver’s Privacy Protection Act prevents state motor vehicle agencies from disclosing of “personal information about any individual” obtained in connection with a motor vehicle record (Relyea, 2001, p. 43). These laws demonstrate a desire to protect any personally identifiable records collected by the government.

Other federal laws go beyond agency records, requiring private entities to protect their personal data files from public view. The Cable Communications Policy Act forbids cable services from disclosing personally identifiable information concerning their subscribers, and the Children’s Online Privacy Protection Act blocks commercial websites from disseminating data about users under 13 years of age (Relyea, 2001, p. 44). Additionally, the Gramm–Leach–Bliley Act represents a collective effort between federal government to facilitate the creation of policies to insure the confidentiality of personally identifiable customer information collected by private financial institutions (Relyea, 2001, pp. 50–51). These legislative actions demonstrate a government interest in protecting the public from a release of personally revealing data, no matter how superficially benign the information is.

5. Lack of privacy for FOIA “patrons”

Although the federal government may support privacy legislation protecting the kinds personal information found in FOIA requests, the current statutes and regulations do not protect FOIA patrons. Obtaining personal information through FOIA requestor records is easy to do, and can be quite revealing. A quick internet search using the Google search engine reveals scores of FOIA requestor logs. FOIA request logs can be found easily on the internet (obviating the lack of privacy given to FOIA requestors). Such records can also be obtained via FOIA requests. In other words, if you are looking for a specific FOIA request or requestor, you can obtain the information you need by requesting it from the government. If somebody wants to find information about a particular FOIA requestor, they can make an FOIA request to every federal agency to discover all of the requestor’s FOIA inquiries and information. Finally, FOIA logs are posted, en masse, on websites like *Government Attic*, which collects FOIA request materials and has a whole page dedicated to FOIA logs. Many federal agencies, like U.S. Citizenship and Immigration Services, proactively publish their logs, posting requestor information on their websites. There is even a government-powered FOIA portal where many requests are cataloged and easily searchable. Any internet user can access recent and historic lists of requestor information in a single Google search or a quick scan of *Government Attic* logs.

FOIA request requirements vary a little by agency, but at the very least, the requestor’s contact information, entity affiliation and request content appear on the log. Sometimes, additional information, including how the request was made, the cost of the request, and detailed writing about the subject of the request also appear.

For example, in a very quick search on the *Government Attic* website’s FOIA log archives, I gathered FOIA request information that revealed requestors’ personal information. These included an FOIA request made by David Gelber at CBS for “Allegations against, and investigations of, high-ranking Mexican officials – cabinet level and above – concerning money laundering and other corrupt activities (including but not limited to drug trafficking, bribery, extortion, and murder),” and a request revealing that the law firm Arent Fox wanted “documents concerning or related to Implementation of WTO

recommendations concerning EC-MEASURES concerning Meat and Meat Products (Hormones).” (FOIA Logs for the Office of the U.S. Trade Representative, 1999–2004). These FOIA request logs information could hint at upcoming news stories, potential lawsuits, and reveal where people work and what they are doing on a given day.

More eerily, I was able to find FOIA requests I made while employed by a law firm. Using my maiden name, I was able to easily discover a collection of FOIA requests made for a (confidential) litigation matter in a Google search (FOIA Logs for the US Securities and Exchange Commission (SEC) 2008–2011 (SEC), 2008–2011, 2012). I felt uncomfortable knowing that, had someone wanted to find out where I worked, how I could be contacted, or what kind of litigation my law firm was involved in, they could run a simple Google search for my FOIA requests. Luckily, I made the requests under my personal name, rather than the name of the law firm in which I was employed, or even worse, the name of a party represented in litigation.

Unsettling at the least, this material could lead to privacy issues for individual requestors and business consequences for requesting entities. For example, the CBS news reporter’s request could have given a competing news corporation information to beat CBS to the story, and revealing a law firm’s interest in particular information could indicate a pending lawsuit or preparation for a case.

Because the FOIA is focused on quick turnaround of information, there is no delay in current information potentially reaching public eyes. Agencies work to avoid FOIA request backlogs, so information is delivered as quickly as possible. In fact, each agency is required to have a special backlog reduction plan to assure that information is delivered at a fast pace (Guidance on preparing backlog reduction plans, 2008).

In 1985, prior to the explosion of internet use, the Department of Justice speculated that requestor’s names are not private enough to be withheld. “In most cases the release of a name of a FOIA requester would not cause even the minimal invasion of privacy required to trigger the balancing tests of [FOIA] exemptions 6 and 7(c).” (United States Department of Justice, 1985).

However, even in 1985, before the pastime of “internet stalking” came of age, the Department of Justice did recognize potential issues related to personal information in FOIA requests could create privacy issues. The Department stated that additional information about the requestor does constitute a privacy concern and “should be protected under Exemption 6 absent a particularly compelling public interest in its disclosure.” (United States Department of Justice, 1985). They listed personal addresses one example of requestor information that should not be revealed in public FOIA request logs. Despite the Department of Justice’s recognition that requestor information should be exempted from the FOIA, in the current system, no law assures that such information is protected.

5.1. The current state of FOIA requestor privacy

With the FOIA’s concentration on transparency, there are not very many limits to information disclosure under the law. FOIA requestor information and request details do not fall under any of the existing FOIA exemptions, and there is no explicit rule protecting the requestors. The U.S. Department of Justice (DOJ) has created an in-depth manual regarding practices and determinations made regarding the FOIA. The DOJ’s *Guide to the Freedom of Information Act* (2009) addresses the topic of FOIA requestors, but does not discuss the privacy rights of those requestors or the exemption of their personal information from FOIA discovery. Requestors do not have to “justify or explain their reasons for making requests” and are highly encouraged to participate in the FOIA process (DOJ, 2009 p. 44).

Case law construes the federal Act’s treatment of requestors and defines the FOIA’s exemptions. The *National Archives and Records Administration v. Favish* (2004), court held that requestors do not have to offer rationales for their FOIA requests. “[W]hen documents

are within FOIA’s disclosure provisions, citizens should not be required to explain why they seek the information.” (*National Archives and Records Administration v. Favish*, 2004, p. 172).

Only a limited body of case law protects FOIA requestors, to some extent, but not directly. *Silets v. U.S. Department of Justice* (1991), is a case in which the court determined that it was proper to redact the requestor’s name from an FOIA request by a high school student seeking government records on the wiretapping of Jimmy Hoffa. The Federal court’s used the exemption under Section 552(b)(7)(C) of FOIA to protect the requestor in this instance. This exemption protects “records or information compiled for law enforcement purposes...to the extent that the production...could reasonably be expected to constitute an unwarranted invasion of personal privacy.” The court reasoned that, in this case, redacting requestor’s name and other identifying information does not affect the public’s understanding of FBI surveillance of Jimmy Hoffa, so using (b)(7)(C) to protect the privacy of the requestor “logically fits within the privacy exception” (*Silets v. U.S. Department of Justice*, 1991, p. 230).

Another federal Court found the identities of private citizens complaining to the FTC about bogus charges on their credit-cards to be exempt from FOIA under a personal privacy exemption (*The Lakin Law Firm, P.C. v. Federal Trade Commission*, 2004). The court found that 5 U.S.C. Section 552(b)(6), which protects “personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy”, applies to these private citizens. “When people feel so strongly about something that they actually complain about it to a federal agency, they probably think their names and addresses will not be released to a firm of private lawyers seeking fuel to propel a possible class-action lawsuit.” The court writes, “Personal identifying information is regularly exempt from disclosure. And that is as it should be, for the core purpose of the FOIA is to expose what the government is doing, not what its private citizens are up to.” (*The Lakin Law Firm, P.C. v. Federal Trade Commission*, 2004, p. 1123).

Despite some success protecting requestors in the courts, federal agencies have been instructed to favor disclosure when considering FOIA exemptions. President Obama recently published an Executive Order requiring a presumption of disclosure of information held by government agencies. He emphasized, “The Freedom of Information Act should be administered with a clear presumption: In the face of doubt, openness prevails.” (*Obama and Memorandum for the heads of executive departments and agencies*, 2009). The executive order acknowledges a profound national commitment to ensuring an open Government, and directs agency FOIA officers to “adopt a presumption in favor of disclosure”.

The only statutory safeguard (aside from the limited FOIA exemptions) that protects information held by federal agencies that reveals information about private citizens is the Privacy Act, although the Privacy Act does not specifically address the privacy of FOIA request information. The Privacy Act regulates the collection, maintenance, use and dissemination of federal agency records pertaining to individual citizens, and limits the collection of records to information needed to carry out agency functions (*Privacy Act of 1974*, 1974). It is designed to protect personal information held by the government, as Congress found it “necessary and proper” to regulate individuals’ personal information held by federal agencies to protect fundamental Constitutional rights of private citizens.

5.2. FOIA “requestors” and library “patrons”

Although library patrons and FOIA requestors seek information in different ways, they are substantially the same in intent and scope. Both a person visiting a library and a person requesting a government document want answers to questions. The essence of the question, be it a reference inquiry, documents from a print or online source, or an

informational request from a government agency, remains the same, and is, basically, “I want to know more.”

Librarians seriously consider their positions as disseminators of information to the public. After the FBI tried to track the library habits of the “Harrisburg Seven”, the American Library Association approved a Resolution on Governmental Intimidation that analogized the ethical model of professional confidentiality in librarianship to the standards of “medical doctors, lawyers, or priests.” (Wilson, 1980). The library community knows fostering patrons’ quests for information hinges on adopting a non-prejudicial attitude towards patrons and avoiding patron the discomfort or intimidation of publicly airing details of their requests. Libraries exist so that members of society can increase their knowledge of the world. The purpose of libraries is not to collect information about individuals who visit them.

Similarly, when the government collects information about individuals, whether it is on purpose (the aggregation of Census data, for instance) or incidentally (while assigning social security numbers and carrying out other types of administrative tasks), the government does not do so to broadcast that personal information in a public setting. Although FOIA officers are charged with receiving and processing FOIA requests in a timely manner, they are not directly charged with preserving patron privacy like librarians. The Privacy Act is the law that directs agencies to protect citizens from sharing citizens’ personal data. The laws governing agencies safeguard the personal records of citizens from “actions of some over-zealous investigators, and the curiosity of some government administrators, or the wrongful disclosure and use, in some cases, of personal files held by Federal agencies.” (United States, Senate Report 89-813). Librarians have a written ethical code lacked in the FOIA officer community. Because there is no official rule governing FOIA officer behavior, there is no guarantee to the privacy of FOIA requestor information because it falls outside the parameters of the Privacy Act.

A fundamental argument in favor of requestor privacy in the FOIA is the idea that, like the materials protected by the Privacy Act, requestors’ acts are not government acts, and their publication does nothing to increase government transparency, which is the singular goal of Freedom of Information measures. Although FOIA requests seek government information, the request document itself contains only personal information, and lacks any government work product or writing.

When Attorney William D. Hill of Kirkland & Ellis wrote to the Attorney General of Texas in 1975 regarding Freedom of Information exemptions for circulation records in the state’s laws, he argued that library records were never intended to fall under the state’s FOI laws. Hill opined, “Library circulation records clearly do not reflect the official acts of public officials and employees.” (Kennedy, 1989, p. 737). Like library requests, FOIA requests are not official government acts. While the information sought may be official, the request itself is simply a means of obtaining information. A request comes from the public, and it does not originate in a government body. As Warren and Brandeis (1890) analogized, it could even be said that the request “belongs” to the requestor as the requestor’s intellectual property.

5.3. Dangers of denying privacy to information requestors

Although the activities of FOIA requestors go largely unrecorded, librarians have written about the fear of privacy deprivation as a real dampening force among information seekers. In fact, it has been argued that the dampening effect caused by lack of privacy may stifle American’s constitutional rights. While discussing library records surveillance, Mark K. Wilson wrote, “The recognition of a first amendment right to read and a finding that this right is unduly burdened by disclosure of library circulation records provide an initial basis

for the imposition of constitutional limitations on access to library borrower lists.” (Wilson, 1980).

Constitutional “limitations” on Americans’ right to read are not isolated to materials found in a library. The “right to read” and obtain information, as enunciated by President Obama’s executive order (2009) and the legislative history materials regarding the FOIA, extends to the information sought by FOIA requestors. Supreme Court Justice William Douglas describes the right to read this way:

“The Constitution was designed to keep government off the backs of the people. The Bill of Rights was added to keep the precincts of belief and expression, of the press, of political and social activities free from surveillance.... When an intelligence officer looks over every nonconformist’s shoulder in the library, or walks invisibly by his side in a picket line, or infiltrates his club, the America once extolled as the voice of liberty heard around the world no longer is cast in the image which Jefferson and Madison designed....” (Laird v. Tatum and 408 U.S. 1, (1972)).

Several published library anecdotes demonstrate the stifling effect of lack of privacy (whether real or perceived) on requestors seeking information. In a Brooklyn, New York library, a patron phoned the local library to see whether they had proceedings from a recent Soviet Communist Party Congress. Although she wanted to look at the publicly available proceedings, she was afraid to come into the library to view them. She asked the librarian, “If I come in and ask for that material, will you report me to the FBI?” (Seeking spies: FBI visits local libraries in effort to recruit informers, 1988).

Requested materials may be provocative, but assumptions about requestors’ rationales can be hasty conclusions that imperil personal freedoms. For instance, a Seattle woman was accused of poisoning her husband’s Excedrin, ultimately killing him. Proof used against her included evidence that she had been reading a library book containing information about cyanide. Although the prosecution used the book as evidence to substantiate their poisoning theory, the woman claimed that she borrowed the books to be sure that plants on her rural property could not harm her grandchildren, whom she watched at her home (Poison pill trial winding to a close, 1988).

Because of the parallels between library patrons and FOIA patrons, the government should be wary of internal systems that publish requestor information. Like FOIA requestors, “People read books for an infinite variety of reasons, and drawing generalized conclusions from another’s reading choices wrongly assumes that the most obvious reason is always the correct one.” (Robertson, 2011, p. 308). FOIA requestors face similar scrutiny about the things they request from the government. A 2008 article estimates that “In approximately three dozen cases since 1975, government entities used [access-to-information statutes] to sue citizens and media outlets that requested access to government information.” (Packer, 2008).

When Judith Krug testified before the Senate Committee during the hearings regarding the VPPA, she argued that intellectual freedom has two inseparable rights. One right springs from the First Amendment, and gives citizens the “right to seek and obtain access to all publicly-available ideas and information.” The other right is the “right to have what one has sought and what one has used kept private.” (United States. Congress. Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the House Committee on the Judiciary and Subcommittee on Technology and the Law of the Senate Committee on the Judiciary, 1988). Krug urges people to avoid inhibiting reading and research interests by allowing them to become public without the reader’s consent. She sites lists of examples of instances where library records have been pursued, including an instance in which the Whitestown, New York police department requested all library patron records covering four years where patrons checked out materials

about “Satanism and the occult” (Statement of Judith F. Krug). This library request is similar to Congressman Issa’s FOIA request for all records from a certain period of time in that it throws a large net over a vast swath of personal information and opens it to public scrutiny. Krug testified in favor of requestor protection:

“There are people in every community who believe that a person’s interest in a subject must reflect not merely his intellectual interests, but his character and attitudes. Thus, in the view of some people, a person who reads the “underground press” is branded a radical; a person who reads atheistic tracts is marked an atheist; a person who reads sexually oriented literature is identified as a libertine.... Such characteristics are not justified or warranted by such literary pursuits but if charged, they can be personally and professionally damaging.”

The FOIA guide (DOJ, 2009) emphasizes that “FOIA request can be made for any reason whatsoever; because the purpose for which records are sought has no bearing upon the merits of the requests, FOIA requesters do not have to explain or justify their requests.” However, there is no guarantee that those requests won’t be used against the requestors. How can requestor neutrality and motive immateriality matter at the asking stage of a request but not after the same request is completed?

North Carolina Senator and longtime civil liberties advocate Sam Ervin, in the Senate Hearing regarding the merits of the Privacy Act of 1974, said:

“Americans are more concerned than ever before about what might be in their records because Government has abused, and may abuse, its power to investigate and store information. They are concerned about the transfer of information from data bank to data bank and black list to black list because they have seen instances of it. They are concerned about intrusive statistical questionnaires backed by the sanctions of criminal law or the threat of it because they have been subject to these practices over a number of years.”

Things like personal reading habits and searches for particular reading materials can open a window into someone’s mind and offer glimpses into their private lives. An ex-bookstore employee described the rationale of their in-house privacy policy:

“Never comment on a customer’s book purchase when completing a sale, for fear that such comments could stifle a customer’s reading habits simply by making the customer aware that another person was privy to information that was possibly personal or embarrassing. Even positive comments were forbidden. After all, letting a customer know how much I enjoyed a novel place conspicuously on top of her stack of books would soon turn awkward if the book underneath the novel was *A Parent’s Guide for Suicidal and Depressed Teens*.” (Robertson, 2011).

Although these anecdotes come from a library setting, there is evidence that in the modern era of online and digital record keeping, government privacy issues are more likely to emerge. As national security concerns lead to laws that strip away personal privacy and erode “information rights,” and the digital collection of personal data expands, the likelihood of a clash between privacy and information collection in a government setting increases (Caidi & Ross, 2005). In the post 9/11 era, “information can be equated with a weapon with the potential to harm any free, open, and democratic nation.” Additionally, “The war on terror encompasses a war on disclosure and dissemination of any information deemed sensitive or having the potential to be used against America. Once overlooked, “under-the-radar” information about people’s whereabouts, intentions, and activities are now potentially

weapon-grade revelations due scrutiny and surveillance (Caidi & Ross, 2005, p. 664).

At the same time that our privacy is being statutorily reduced by laws like the USA PATRIOT Act, the government is collecting more personal information about its citizens. In 2009, the United States Government Office of Management and Budget (OMB) decided to change its prohibition on web tracking technologies, like cookies, on federal websites (McCarthy & Yates, 2010). The OMB said that decreasing privacy to allow the use of social media services would make federal government websites “more user friendly, providing better customer service, and allowing for enhanced web analytics,” (McCarthy & Yates, 2010, 232) but pro-privacy organizations including the American Civil Liberties Union, the Electric Privacy Information Center, and the Electronic Frontier Foundation challenged the removal of the cookies prohibition as a potential reversal on the existing policy assuring that government websites should not be able to track the internet use activity of government website users (Electronic Frontier Foundation, 2009).

As the government weakens its internet privacy policies, technology makes it easier to obtain information quickly. Michelle G. Hough (2009) describes the breakdown of privacy as a loss of “reserve,” or the loss of anonymity (defined by Hough as “the ability to distance oneself from public interest”) through decreased control of personal information (Hough, 2009, p. 407).

Hough uses grocery store loyalty cards to illustrate the loss of reserve. First, Hough reviews old methods of collecting personal information, in which the information compiler “would need to make separate visits to hospitals and physicians, to any schools the individual may have attended, to former places of employment, to banks and other possible places of business, and to law enforcement agencies in any locations where the individual lived or likely spend time” and speak with real human beings at each location. She then illustrates the ease of modern information collection by showing that, with a swipe of a loyalty card by a cashier, “The cards link to databases which store standard customer information: name, address, date of birth, possibly even Social Security of bank information, if connected to check-cashing privileges... They can also record every item purchased by that consumer.” These records can be used for all sorts of purposes, even legal ones. For instance, “A supermarket in California used shopper loyalty information to assert that a customer who was injured in their store probably was impaired at the time of the accident, given the quantity of liquor the customer regularly purchased there.” (Hough, 2009, p. 408).

These modern quick data collection methods are not only for grocers. Government agencies also use them, and private information often ends up in government files with only begrudging consent. Most individuals have no choice but to feed information to agencies like the Internal Revenue Service, the Social Security Administration, the Census Bureau, Medicare, and other government authorities (Gayton, 2006). With the increasing ease of personal data collection comes the increasing need to legislate privacy protections to prevent the breakdown of privacy rights. As the Electronic Frontier Foundation explains, “the law has yet to catch up to our evolving expectations of and need for privacy. In fact, new government initiatives and laws have severely undermined our rights in recent years.” (EFF, 2009). This need for privacy legislation extends to all facets of government, and it includes the goal of safeguarding the FOIA to protect FOIA requestors in a climate where increased surveillance and decreased privacy reserve make personal information ever more valuable and easy to use.

6. Conclusion

The goal of FOIA is not to hide information, but to reveal it. However, a line must be drawn in revealing government information to the public to protect those requesting the information, in order to

keep the flow of information open and the government a welcoming center for inquiry. As one person worried about Congressman Issa's request for volumes of FOIA records stated, "it seems sort of creepy that one person in the government could track down who is looking into what and what kinds of questions they are asking." (Lipton, 2011). Basic rights to privacy, developed through eras of political turmoil and volumes of legal theory and practice, protect the discovery of people's personal inquiries and requests. Anything that deters people's right to ask questions of the government is to be avoided under historical and contemporary American legal jurisprudence (Caidi & Ross, 2005).

Librarians have a model set of ethical guidelines and practices for dealing with requestors' privacy. They protect circulation records, going so far as to dispose of them to avoid their discovery by outsiders. Reference librarians regard their transactions with library patrons as confidential. Libraries' ethical boundaries could serve to inform the Federal government when dealing with requests from members of the public.

Using state laws that protect the confidential information of library patrons as a model, the federal government could draft statutory protections for FOIA requestors. If the federal government treated FOIA requestors with the level of privacy afforded library patrons, they could guarantee the protection of American's constitutional rights when they seek information. The ALA values privacy rights as much as ever, proving that, especially in this electronic era, we must all take extra steps to assure the privacy of information requestors.

Acknowledgment

The author wishes to thank Eyal Benjamin, Benjamin Lamdan, Evelyn Lamdan, Douglas Cox, Babe Howell, Yasmin Sokkar Harker, Raquel Gabriel, Alex Berrio Matamoros, and Keith Szczepanski for their assistance and support during the drafting and editing of this article. She would also like to heartily thank the CUNY School of Law faculty and staff, especially Director of the Law Library, Julie Lim, and members of the library staff for their tremendous support as mentors and colleagues in the profession of law librarianship.

References

- Abernethy v. Hutchinson, (1825) 26 Eng. Rep. 1313 (Ch.).
 Ala. Code § 41-8-10 (2011).
 American Library Association Office for Information Technology Policy (2012). Retrieved 11/14, 2012, from <http://www.ala.org/offices/oitp>
 American Library Association Office For Intellectual Freedom (2005). *Intellectual freedom manual* (8th ed.). Chicago, IL: ALA Editions.
 Ark. Code Ann. § 13-2-701 (2011).
 Ark. Code Ann. § 13-2-703(b) (2011).
 Bloustein, E. J. (1968). Privacy, tort law, and the constitution: Is and Brandeis' tort petty and unconstitutional as well? *Texas Law Review*, 46, 611.
 Caidi, N., & Ross, A. (2005). Information rights and national security. *Government Information Quarterly*, 22, 663–684.
 Citizen Advocacy Center (2008). Accessing government: How difficult is it? An analysis of open government laws in the Midwest. Retrieved 11/14, 2012, from <http://www.citizenadvocacycenter.org/OGP.html> (Colo. Rev. Stat. § 24-72-204(3) (2011))
 Cooley, T. M. (1868). *A treatise on the constitutional limitations which rest upon the legislative power of the states of the American union*. District Court of the District of Massachusetts: Little, Brown and Company.
 Cooley, T. M. (1880). *A treatise on the law of torts, or, the wrongs which arise independent of contract* (2nd ed.). Chicago, IL: Callaghan & Company.
 Coolidge, K. K. (2005). "Baseless hysteria": The controversy between the Department of Justice and the American Library Association over the USA PATRIOT Act. *Law Library Journal*, 97, 18.
 Coyle, K. (2002). Make sure you are privacy literate. *Library Journal*, 127, 55.
 Department of Justice v. Reporters Commission For Freedom of Press, 489 U.S. 749 (1989).
 Electronic Frontier Foundation (2009). *Letter to White House Counsel*. What will you do to protect the privacy of Whitehouse.gov users? (Retrieved 11/14, 2012, from <https://www.eff.org/deeplinks/2009/01/eff-white-house-counsel>)
 Finkelman, P. (Ed.). (2006). *Encyclopedia of American civil liberties*. New York, NY: Routledge.
 Fla. Stat. § 257.261 (2011).
 FOIA Logs for the US Securities and Exchange Commission (SEC) 2008–2011 (2012). Retrieved 11/14, 2012, from http://www.governmentattic.org/4docs/SEC-FOIA-Logs_2008-2011.pdf
 FOIA Logs for the Office of the U.S. Trade Representative (1999–2004). Retrieved 11/14, 2012, from http://www.governmentattic.org/docs/FOIA_Logs_USTrade_Representative_1999-2004.pdf
 Garoogian, R. (1991). Library/patron confidentiality: An ethical challenge. *Library Trends*, 40, 216.
 Gayton, C. (2006). Beyond terrorism: Data collection and responsibility for privacy. *VINE: The Journal of Information and Knowledge Management Systems*, 36, 377–394.
 Griswold v. Connecticut, 383 U.S. 479, 482 (1965).
 Guidance on preparing backlog reduction plans (2008). United States Department of Justice office of information and privacy FOIA post. Retrieved 12/21, 2012, from <http://www.justice.gov/oip/foiapost/2008foiapost22.htm>
 Harris v. Blockbuster, No. 2:08-cv-00155-DF (E.D. Tex. 2008).
 Hough, M. G. (2009). Keeping it to ourselves: Technology, privacy and the loss of reserve. *Technology in Society*, 31, 406–413.
 Jackson, W. (2010). *Guidelines take stab at guarding personal information*. GCN. (Retrieved 12/21, 2012, from <http://gcn.com/articles/2010/04/12/nist-pii-guidelines-041210.aspx>)
 Johnson, B. S. (1989). "A more cooperative clerk": The confidentiality of library records. *Law Library Journal*, 81, 796.
 Kennedy, B. M. (1989). Confidentiality of library records: A survey of problems, policies, and laws. *Law Library Journal*, 81, 733.
 La. Rev. Stat. Ann. § 44:13 (2011).
 Laird v. Tatum, 408 U.S. 1 (1972).
 Lamdan, S. S. (2012). Protecting the Freedom of Information Act requestor: Privacy for information seekers. *Kansas Journal of Law & Public Policy*, 21, 221.
 Letter from Darrell E. Issa, Chairman, House Committee on Oversight and Government Reform, to FOIA Officers (2011). Retrieved 11/14, 2012, from graphics8.nytimes.com/packages/pdf/politics/20110129-issa.pdf
 Lipton, E. (2011). Republican congressman proposes tracking Freedom of Information Act requests. *The New York Times* (pp. A14).
 Matz, C. (2008). Libraries and the USA Patriot Act: Values in conflict. *Journal of Library Administration*, 47, 69–72.
 McCarthy, L., & Yates, D. (2010). The use of cookies in federal agency web sites: Privacy and recordkeeping issues. *Government Information Quarterly*, 27, 231–237.
 Milans v. Netflix, Inc., No. 5:2011-cv-00379 (N.D. Cal. 2011).
 N.M. Stat. Ann. § 18-9-2 (2010).
 National Archives & Records Administration v. Favish, 541 U.S. 157 (2004).
 Obama, B. H. Memorandum for the heads of executive departments and agencies. (2009). Presidential memoranda. Retrieved 12/21, 2012, from http://www.whitehouse.gov/the_press_office/Freedom_of_Information_Act
 Ostrowsky, B. (2005). Anonymous library cards allow you to wonder, 'who was that masked patron'? *Computers in Libraries Magazine*, 25, 21–22.
 Packer, C. (2008). Don't even ask! A two-level analysis of government lawsuits against citizen and media access requestors. *Communication Law and Policy*, 13, 29.
 Peltz, R. J., Joi, L. L., & Andrews, A. J. (2006). The Arkansas proposal on access to court records: Upgrading the common law with electronic freedom of information norms. *Arkansas Law Review*, 59, 555–706.
 Poison pill trial winding to a close (1988). New York Times. Retrieved on 12/21, 2012, from <http://www.nytimes.com/ref/membercenter/nytarchive.html>
 Pollard v. Photographic Co., (1888) 40 L.R. Ch.D. 345 (Ch. D.).
 Presidential statement on signing S. 1160, the Freedom of Information Act of 1966 (1966). *Weekly compilation of presidential documents*, 2. (pp. 895).
 Presidential statement on signing the Electronic Freedom of Information Act amendments 1996 (1996). *Weekly compilation of presidential documents*, 32. (pp. 1949).
 Prince Albert v. Strange, (1849) 64 Eng. Rep. 293 (Ch.).
 Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974).
 Public Inspection of Public Library Records, Op. Att'y Gen 82-149. (1982). Frankfort, KY: Office of the Kentucky Attorney General.
 Raymond, M. (2010). How tweet it is!: Library acquires entire Twitter archive. *Library of Congress blog* (Retrieved 12/21, 2012, from <http://blogs.loc.gov/loc/2010/04/how-tweet-it-is-library-acquires-entire-twitter-archive/>)
 Regan, P. M. (2004). Old issues, new context: Privacy, information collection, and homeland security. *Government Information Quarterly*, 21, 481–497.
 Relyea, H. C. (2001). Legislating personal privacy protection: The federal response. *The Journal of Academic Librarianship*, 27, 36–51.
 Robertson, E. (2011). A fundamental right to read: Reader privacy protections in the U.S. constitution. *University of Colorado Law Review*, 82, 307–308.
 Sevy v. Netflix, Inc., No. 5:2011-cv-01309 (N.D. Cal. 2011).
 Silets v. U.S. Department. of Justice, 945 F.2d 227 (1991).
 Solove, D. J. (2011). *Why privacy matters even if you have 'nothing to hide'*. *The Chronicle of Higher Education*. (Retrieved 12/21, 2012, from <http://chronicle.com/article/Why-Privacy-Matters-Even-if-127461/>)
 Stanley v. Georgia, 394 U.S. 557 (1969).
 Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044 (Co. S. Ct. 2002).
 The Freedom of Information Act of 1966, 5 U.S.C. § 552. (2010).
 The Lakin Law Firm, P.C. v. Federal Trade Commission, 352 F.3d 1122, 1124 (7th Cir. 2004).
 United States Department of Justice (1985). FOIA counselor: Questions & answers. *FOIA update*, 6. (pp. 4) (Retrieved 12/28/2012, from http://www.justice.gov/oip/foia_updates/Vol_VL_1/page4.htm)
 United States Department of Justice (2009). Guide to the Freedom of Information Act. Retrieved 12/27/2012, from http://www.justice.gov/oip/foia_guide09.htm
 United States. Congress. Senate. Committee on the Judiciary (1965). Clarifying and protecting the right of the public to information, and for other purposes. *Senate report 89-813*. Washington DC: Government Printing Office.

- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107–56, 115 Stat. 272 (2001).
- Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(193), 205.
- Wilson, M. K. (1980). Surveillance of individual reading habits: Constitutional limitations on disclosure of library borrower lists. *The American University Law Review*, 30, 275.
- Wis. Stat. § 19.35(1)(a)(i) (2008)).
- Zalusky, S. (2011). *ALA council continues opposition to use of section 215 of Patriot Act and use of national security letters to violate reader privacy. American libraries* (Retrieved 12/12, 2012, from <http://americanlibrariesmagazine.org/news/ala/ala-council-continues-opposition-use-section-215-patriot-act-and-use-national-security-lett>)

Sarah Lamdan, Associate Law Library Professor, received her J.D. from the University of Kansas School of Law with a Certificate in Environmental and Natural Resources Law, a Master's Degree in Legal Information Management from Emporia State University's Graduate School of Library and Information Management, and a B.A. in English from the University of Kansas. She previously served as research librarian for several international law firms.

Her research interests include the Freedom of Information Act, administrative law, environmental law, and environmental justice topics, especially those pertaining to information access issues. She recently authored "Protecting the FOIA requestor: Privacy for information seekers," which appears in the Spring, 2012 edition of the *Kansas Journal of Law & Public Policy*, and she has served as a panelist and information ethics and social media ethics events. She is a member of the Law Librarian Association of Greater New York (LLAGNY) and of the American Association of Law Libraries (AALL).