2014

Intellectual Freedom and Privacy

Neil M. Richards
Washington University in St. Louis School of Law, nrichards@wustl.edu

Joanna Cornwell

Washington University in St. Louis
SCHOOL OF LAW

Intellectual Freedom and Privacy

Neil M. Richards[1] & Joanna F. Cornwell[2]

Adapted from Mark Alfino, Ed., The Handbook of Intellectual Freedom (Unwin, 2014).

INTRODUCTION

Intellectual freedom and privacy are distinct concepts, but they are related and mutually reinforcing. Certain kinds of privacy protections can be essential to the meaningful exercise of intellectual freedoms. Particularly when individuals are engaged in intellectual activities (broadly defined), privacy protections can operate to provide a shield from the scrutiny and interference of others so that intellectual inquiry – thinking, reading, and private conversations – can occur. The absence of such protections for

[1] Professor of Law, Washington University School of Law.

[2] J.D. 2013, Washington University School of Law.

Word Count: 7,265 words, incl. footnotes

"intellectual privacy" (whether physical, social, or legal) can shine the light of surveillance onto intellectual activities, driving them to the conventional, the mainstream, and the uncontroversial. (Richards 2013a; 2013b, 2008).

Americans have long understood the links between a well-educated citizenry and the preservation of democratic self-government. (ALA 2012c). For example, Benjamin Franklin started the first public subscription library in 1731 in Philadelphia, Pennsylvania (Morse 1989). Nine signers of the Declaration of Independence were members of Benjamin Franklin's Library Company. (Library Company 2012). Modern librarians continue this commitment. The American Library Association asserts that intellectual freedom has two main dimensions: 1) "the right of every individual to hold any belief of any subject and to convey their ideas in any form they deem appropriate," and 2) "that society make an equal commitment to unrestricted access to information and ideas." (ALA, 2012c). Legally, the concept of intellectual freedom in the United States is associated with the First and Fourth Amendments of the U.S. Constitution. The First Amendment protects the right of freedom of speech and press, and their associated freedoms of thought, belief, and inquiry. The Fourth Amendment protects an

individual's "persons, houses, papers, and effects" from unreasonable government searches and seizures, and had its genesis in the need to protect private correspondence from government surveillance. As William Stuntz has explained, the origins of the Fourth Amendment have much in common with the origins of the First. Stuntz has shown how the eighteenth century British Crown frequently used criminal prosecutions for seditious libel to suppress dissidents and other government critics, and used searches of private property for diaries and other incriminating texts in order to advance such prosecutions. Such prosecutions were also common in the colonies, and formed the context out of which the Fourth Amendment was drafted and ratified. (Stuntz 1995). From this perspective, the First Amendment protects the right to speak, while the Fourth protects the ability to develop ideas away from the interference of the state. Both protections thus work together to guarantee intellectual freedom as a constitutional matter.

Modern understandings of intellectual freedom reflect these constitutional origins. The First Amendment's protections extend beyond those of speakers to those of listeners as well, and include the right to know or receive information. (Emerson 1976; Solove &

Richards 2009). The right to know is an important liberty because it provides individuals with the ability to seek the truth, to aid collective decision-making for political processes, and to obtain personal fulfillment (Emerson 1976). Moreover, the right of free speech also includes the right to speak anonymously or under a pseudonym, a well-established practice in American public debate since James Madison, John Jay, and Alexander Hamilton penned *The Federalist* under the pseudonym Publius. Readers and listeners of public speech may similarly want to remain anonymous and to consume this information in a quiet space (such as a library) without observation (Blitz 2006). It is in such contexts that privacy has the most meaningful role to play in providing protection for intellectual pursuits.

Privacy is a wide-ranging, complex concept and it continues to change as information technology and social norms evolve (Nissenbaum 2004; Solove 2010). The first well-known legal definition of privacy came from the 1890 Warren and Brandeis article "The Right to Privacy," which famously defined privacy as the "right to be let alone" (Warren & Brandeis 1890). In response to this article, state legislatures and courts created or recognized privacy rights as a matter of state tort law. These decisions were

ultimately categorized into four distinct torts by William Prosser during the middle decades of the twentieth century, and through Prosser's influence over the course of tort law most jurisdictions today recognize four separate causes of action under the right to privacy: intrusion into seclusion, disclosure of private facts, appropriation of likeness, and false light (Richards & Solove 2010).

While the tort law of privacy has remained relatively stable, scholarly understandings of privacy have continued to evolve as legal scholars have subsequently developed new analytic frameworks to better understand what privacy can mean. Moreover, the emerging world of information and electronic communications technologies has placed increased importance on the idea of privacy. Scholarly understandings of "information privacy" have struggled with the definition of privacy and the values it protects. Responding to the first "data bank" technologies in the 1960s, Alan Westin argued that privacy is not an absolute right, but rather a claim for individuals and institutions "to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin 1967). Westin's intuitive understanding of privacy as having something to do with control over one's personal information remains influential in today's

scholarly and policy understandings of privacy. However, definitions of privacy have remained elusive.

Two recent conceptual advances are also worthy of mention. First, Daniel Solove has offered a four part "taxonomy" of information privacy (Solove 2010). Solove divides harmful activities in information privacy into the four principal categories of 1) information collection, 2) information processing, 3) information dissemination, and 4) invasion (Solove 2010). Solove proceeds to break down these four parts into more specific harmful sub-activities. Information collection involves surveillance and interrogation, or probing for information (Solove 2010). Information processing describes how outside entities such as the government and businesses process and manipulate an individual's data by engaging in the following activities of aggregation, identification, insecurity, exclusion, and secondary use (Solove 2010 104) Information dissemination describes what happens to an individual's data when it is shared with third parties, including potentially: breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation and distortion (Solove 2010). Finally, invasion details the specific harm to an individual's privacy, namely intrusion into their tranquility and

decisional interference (Solove 2010). While Solove admits these categories are artificial, he advocates for a bottom-up approach to examining privacy problems (Solove 2012). By using this approach, privacy problems will not be overlooked and privacy principles will be better informed to understand such privacy problems in the first place (Solove 2012).

Also recognizing the difficulty in defining privacy, Helen Nissenbaum provides three principles for guiding contemporary privacy policy: "1) limiting surveillance of citizens and use of information about them by agents of government, 2) restricting access to sensitive, personal, or private information, and 3) curtailing intrusions into places deemed private or personal" (Nissenbaum 2004). In subsequent work Nissenbaum notes that few people actually want their information to be kept confidential under all circumstances, but rather that most people want their information to flow, but to flow within appropriate norms. These norms, she asserts, vary from context to context, such that the key to sensible privacy policy is to maintain what she calls "contextual integrity" – the appropriate balance between privacy and flow depending on social norms (Nissenbaum 2010).

In this essay, we provide an account of the ways in which intellectual freedom and privacy are interrelated. We pay particular attention to both the constitutional dimensions of these important values, as well as the important roles that social and professional norms play in their protection in practice. Our examination of these issues is divided into three parts. Part I lays out the law and legal theory governing privacy as it relates to intellectual freedom. Part II examines a special context in which law and professional norms operate together to protect intellectual freedom through privacy – the library. Finally, Part III discusses how government actions and other threats can infringe individuals' privacy, potentially threatening intellectual freedom.

I. PRIVACY LAW AND INTELLECTUAL FREEDOM

A. First Amendment Theory and Intellectual Freedom

The First Amendment's guarantees of free speech and press protect many things, but at their core is a commitment to intellectual freedom. We can see this commitment in the seminal free speech texts from the early twentieth century, texts which have become the core of First Amendment theory today (Richards 2008). For example, Justice Oliver Wendell Holmes' famous dissent in

Abrams v. United States quite clearly linked the purposes of constitutional protection free speech with the search for truth, a statement of intellectual freedom in its most stark and philosophical form. The underpinnings of intellectual freedom in First Amendment theory can be seen even more clearly in Justice Brandeis' opinions in *Whitney v. California* and *Olmstead v. United States*. In *Whitney*, the Court was examining the constitutionality of California's criminal syndicalism statute under the First Amendment. In Justice Brandeis' concurrence, he noted that:

> Those who won our independence believed that the final end of the state was to make men free to develop their faculties . . . . They believed that freedom to think as you will and to speak as you think are means indispensable to the discovery and spread of political truth (Whitney 1927).

Although Brandeis' opinion did not have the effect of law when it was published, over time it has been recognized by courts and legal scholars as one of the most important statements regarding how the First Amendment should be protected, and why it should be protected broadly to promote intellectual freedom. In

Whitney, Brandeis was not merely making a historical comment on our nation's founders, but rather was describing how essential freedom of speech is to self-government (Richards 2010). In order to have an effective self-government resulting in more democratic decisions, there must be an educated and democratic citizenry (Richards 2010). The recognition of how critical free speech is to producing an informed, educated and democratic citizenry is one of Brandeis' most innovative and novel contributions to First Amendment jurisprudence (Richards 2010). A democratic citizenry must have robust free speech protections and access to new opinions, as what lawyers call "counter-speech" is the best remedy to dangerous and harmful ideas (Richards 2010). Brandeis describes this concept:

> "If there be time to expose through discussion the falsehood and fallacies, to avert the evil by the process of education, the remedy to be applied is more speech, not enforced silence." (Whitney 1927).

Brandeis' connections between free speech, self-government, a democratic citizenry, and intellectual freedom have since become

a cornerstone of modern First Amendment speech theory (Richards 2010). Brandeis further explained the linkages between privacy and intellectual freedom in his well-known dissent in *Olmstead v. United States* (1928). (Richards 2008; Richards 2010). *Olmstead* was a Fourth Amendment case in which the majority of the Supreme Court held that federal wiretapping did not require a warrant under the Fourth Amendment. Brandeis argued that:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone - the most comprehensive of rights and the right most valued by civilized man (Olmstead 1928).

Brandeis' dissenting arguments in *Olmstead* eventually carried the day, and his arguments were accepted by the Supreme Court in *Katz v. United States* (1967), which ruled that the Fourth

Amendment protects a person's "reasonable expectation of privacy." *Olmstead* was, of course, a Fourth Amendment case, but in his opinion, Brandeis revealed some of the ancient connections between the First and Fourth Amendments in the context of intellectual freedom. Brandeis thus illustrated how privacy could provide a shelter for free thought and intellectual freedom (Richards 2008). He went on to warn prophetically that in the future it might be possible for "the government, without removing papers from secret drawers, [to] reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions." (Olmstead 1928). In order to prevent this, Brandeis argued, novel and unjustifiable intrusions into domestic and intellectual privacy must be considered a violation of the Fourth Amendment.

Brandeis's connections between privacy and freedom of speech nevertheless run somewhat against the grain of the traditional ways that courts have approached the relationship between these two values. Traditionally, the Supreme Court and First Amendment scholars have considered privacy as a hostile or

competing value to free speech. This typically occurs when a privacy cause of action is brought against the press for disclosing true but newsworthy facts about the subject of a news story (Richards 2008). In such cases, the Supreme Court usually holds that the constitutional right of free speech under the First Amendment value prevails against the tort right in protecting one's emotions from distress (Richards 2008). Most recently for example, in *Snyder v. Phelps*, the Court examined an invasion of privacy claim by a deceased military veteran's father subjected to horrific anti-gay protesting by the Westboro Baptist Church at his son's funeral (Snyder 2011). The Court held that the veteran's father did not prove the elements for an invasion into privacy tort and that the First Amendment "protect[s] even hurtful speech on public issues to ensure that we do not stifle public debate" (Snyder 2011). A long line of earlier cases have held that the First Amendment protects the ability of the press to publish emotionally damaging but true statements, such as the names of rape victims notwithstanding civil and criminal laws to the contrary (Richards 2011).

Notwithstanding these precedents, privacy is able to survive challenges from the First Amendment when it protects spaces or

relationships from intrusion (Richards 2011). This is especially the case when government actors are the ones seeking to intrude, as the robust body of Fourth Amendment law protecting the privacy of the home can attest to. Thus, in *Kyllo v. United States*, the Court held it to be a violation of the Fourth Amendment when the government had used an infrared thermometer to measure the temperature of the exterior of a house they suspected was harboring an indoor marijuana farm. And in *Wilson v. Layne,* the Court also found a violation where police brought a reporter along with them to observe the execution of an arrest warrant in a private home. The Court has also on limited occasions recognized that the First Amendment protects intellectual freedom in the privacy of one's home directly. In *Stanley v. Georgia*, the Court famously recognized the right of an individual to read books and watch films, even pornographic films that were otherwise illegal to possess, in the privacy of one's home, against government intrusion. The Court held that:

> If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch. Our whole constitutional

> heritage rebels at the thought of giving government the power to control men's minds (Stanley 1969).

B. Intellectual Privacy

Within First Amendment law and theory, Neil Richards has located and illustrated "intellectual privacy," the "ability, whether protected by law or social circumstances, to develop ideas and beliefs away from the unwanted gaze or interference of others" (Richards 2008). Although intellectual privacy as an identified term is relatively new, its roots in First Amendment theory are much older, and can be traced back to Brandeis and *Stanley*. Intellectual privacy strengthens the right to speech as it provides a theory of protection for the freedom of thought; it protects the way in which our minds develop to say something before the speech actually occurs (Richards 2008). Richards argues the "First Amendment should protect cognitive activities even if they are wholly private and unshared because of the importance of individual conscience and autonomy" (Richards 2008). A theory of intellectual privacy also "creates a screen against such surveillance" as surveillance can chill First Amendment activities when readers in fear of being watched do not access certain articles on the Internet

or do not check out certain books (Richards 2008; Richards 2013a; 2013b).

Legal Scholar Julie Cohen has also recognized the value of intellectual privacy in a number of contexts (Cohen 1996). She notes that "reading is so intimately connected with speech, and so expressive in its own right, that the freedom to read anonymously must be considered a right that the First Amendment protects" (Cohen 1996). Under the current copyright law, there is no obligation for companies to maintain a reader's anonymity when using their product (Cohen 1996). Therefore, she stresses that the law be amended to ensure autonomy-based rights are recognized and provide "breathing space for thought, exploration, and personal growth" (Cohen 2003). In her recent book *Configuring the Networked Self*, Cohen expands this theory, arguing that informal opportunities and spaces for private experimentation allow for the development of the self, whether alone or in the company of others. Cohen notes that intellectual privacy is important not just for high-minded "intellectual" ideas, but also for whatever ourselves wish to experiment with as part of our engagement in the formation of culture – a phenomenon she calls "the play of everyday practice" (Cohen 2012).

Daniel Solove argues that government actions and subpoenas that request reading lists, diaries, internet search histories, computer hard drives, and emails implicate an individual's First Amendment liberties (Solove 2007). Solove proposes that the First Amendment can be used alongside the Fourth and Fifth Amendments as a source of criminal procedure to prevent invasive government intrusion when the intrusion implicates the First Amendment (Solove 2007). He recommends that courts should determine whether or not the First Amendment applies when the government seeks a subpoena for information gathering purposes and then determine if the request would have a sufficient chilling effect on the First Amendment activity (Solove 2007). In the event the First Amendment applies, the court must then determine whether or not the government had "a significant interest in gathering the information, and, if so, whether the process was narrowly tailored to the government interest" (Solove 2007).

C. State Laws on Protecting Reader Privacy

There is no federal statute protecting reader privacy, but 48 states and the District of Columbia have passed library reader confidentiality laws (Klinefelter 2010). The remaining states,

Kentucky and Hawaii, have no express legislative protection of librarian privacy, though their state Attorneys General have each issued opinions declaring that the state protects the privacy of library users (Klinefelter 2010). State library privacy laws vary widely in scope, as some states only protect public libraries, rather than (for example) private university libraries. Operating on top of the state laws are library privacy policies, which can provide higher levels of privacy protection to their patrons. Klinefelter notes that the state may offer more reader privacy protection, a library's own policy may offer the reader more protection, or a reader may be protected by both a state law and library policy (Klinefelter 2010).

Beyond libraries, several states offer protections for reader records generally, such as those created by bookstores and websites, though the type of protections and type of mediums protected also varies widely from state to state (Richards 2013). In Michigan's Preservation of Personal Privacy Act of 1988, all records of selling, renting or lending books and other written materials shall not be disclosed to any third party unless provided by law, broadly defined (MICH. § 445.1712). In California, the Reader Privacy Act of 2012 protects all reading records, including e-books, from disclosure to third parties unless the government has a proper court order or a

private entity has a user's informed and affirmative consent for a specific use of this record (CAL. CIV. CODE § 1799.3). In contrast to other states statutes' providing for reader protection, Colorado protects the right to purchase books anonymously through Article II, Section 10 of its state Constitution (Richards 2013). The Colorado Supreme Court upholds the importance of reader privacy and sets forth a balancing test that requires law enforcement officials seeking specific book records from a bookstore to first demonstrate a compelling government need for these records and the court can consider whether there are reasonable alternative methods of meeting this need, whether the warrant is too broad, and whether the reason for seeking these records are valid (Tattered Cover 2002, 1047). As evidenced by this sample of state protections, the type of reading materials protected and the regulation of disclosure to third parties provides an uneven treatment of reader records under our law (Richards 2013).

II. LIBRARIANS AND INTELLECTUAL FREEDOM

As the previous discussion of library policies suggests, libraries and librarian ethics play a central role in any discussions of intellectual freedom and privacy. Indeed, the professional work of librarians is perhaps the context in which the linkages between

privacy and intellectual freedom have been recognized the most. This is true both as a matter of the theory of librarianship as well as a series of practices and norms that embody these theories into everyday institutions and interactions. As a center for "uninhibited intellectual inquiry," libraries are places where individuals can self-direct their learning towards a collection of books, periodicals, digital information, and other media without bias or scrutiny (ALA 2012c). Courts have also noted that libraries play an important role in providing a citizen with access to the printed word, and more broadly to all ideas (US vs. ALA 2003).

As such, librarians have a long history in advocating for privacy as an instrumental goal in furtherance of their broader commitment to the intellectual freedom of their patrons. The American Library Association (ALA) first affirmed a right to privacy in 1939 (ALA 2002). The ALA Library Bill of Rights outlines the duties and the principles for how librarians should protect and defend intellectual freedom (ALA 2012c). Today, the ALA Code of Ethics states: "[w]e protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted" (ALA 2012b). The ALA believes that the right of privacy ensures an

individual may openly learn, read, and research without intrusion (ALA 2002). When individuals fear surveillance or that their privacy is threatened, the ALA's position is unequivocal that true intellectual freedom no longer exists (ALA 2002).

A. Libraries advocate for protecting a user's confidentiality and personally identifiable information.

While library records have been recently targeted for national security reasons under the USA Patriot Act since 2001, government agencies have been seeking library records in criminal investigations for decades. In response to these government actions, in 1970 the ALA adopted a policy that library records are to be deemed confidential and not considered public records, even for public libraries (ALA 2012c). The ALA's Office of Intellectual Freedom publishes an Intellectual Freedom Manual, which sets forth a policy on confidentiality of library records (ALA 2012c). The Manual states that not only does the Librarian Code of Ethics include a duty to protect the privacy and confidentiality of library patrons, but also that librarians should not release an individual's records to a government agency without an authorized process, order, or subpoena (ALA 2012c). Upon receiving the subpoena, the librarian should consult with legal counsel to determine if the

subpoena is proper and if there is a showing of good cause for its issuance (ALA 2012c). The ALA also recommends that libraries create and publish a privacy policy, so that users are aware of and consent to how their personal information is being collected, used, and stored (ALA 2012c).

B. Library Privacy Policies as Models for the Digital World

By thus making duties of confidentiality and respect for patron reading privacy an important part of the professional ethics of librarianship, the ALA shows how social and ethical norms can place an additional level of privacy protection on top of whatever legal rules might be in place. With the advent of new digital technologies, librarian and legal scholar Ann Klinefelter argues that libraries are confronted with new opportunities for reader records to be shared instead of discarded (Klinefelter 2010). With respect to these online sharing systems, libraries have proceeded cautiously "with a policy of opt-in, rather than opt-out for those services that have the potential to compromise reader privacy" (Klinefelter 2010). Although some librarians might question a need for privacy in a "culture fueled by Facebook, blogs, Twitter and celebrity" or would like to study readers' data for social sciences purposes,

Klinefelter notes that most librarians are "committed advocates for the privacy of thought through reading" (Klinefelter 2010). Moreover, the set of professional rules and practices that librarians have developed to protect free reading and intellectual inquiry could be extended to other areas. Klinefelter suggests that the rules librarians have developed could serve as a model for other digital environments such as Google Books, e-readers, and other digital mediums (Klinefelter 2010, 561). Other legal scholars have made similar arguments (Richards 2013; Blitz 2006; Cohen 1996; 2003).

C. The Advent of Social Reading Applications Threaten Reader Privacy

A new phenomenon on the Internet in recent years has been the rise of "social reading." This is the idea that automatic disclosure of one's friends' reading habits gives Internet users suggestions of new and interesting things to read. Accordingly, companies like Facebook and Twitter, in collaboration with many newspapers, have created "social reading" opportunities for online users (Richards 2013). Once a reader provides a one-time consent to a website newspaper application, then "the application can be used to allow the automatic disclosure of their reader records to

their friends on social networks" (Richards 2013). This automatic disclosure is known as "frictionless sharing." Richards argues that while some sharing may appear to be "cool," there are inherent dangers in frictionless sharing that threaten a reader's intellectual freedom and privacy (Richards 2013). First, frictionless reading is not frictionless as the application can inadvertently invade a reader's privacy when they do not intend to share an embarrassing article that they read by posting the article automatically on their social network page (Richards 2013). Second, frictionless sharing eliminates conscious or meaningful sharing (Richards 2013). Third, frictionless sharing does not guarantee our intellectual freedom will advance, but rather it hinders our ability to freely engage with any ideas "on our own terms with meaningful guarantees that we will not be watched or interfered with" (Richards 2013). If readers are worried that our reading habits might be disclosed automatically or accidentally, then readers would become less likely to engage or experiment with unpopular or deviant ideas.

Richards suggests that social reading applications should build applications based on an opt-in and conscious choice, so that reading is confidential and that sharing an article can be conscious

and valuable (Richards 2013). Although social reading creates significant threats to reader privacy, millions of readers have signed up for reading applications on Facebook in 2012, indicating that some readers enjoy the frictionless sharing application (Purewal 2012). By May 2012, millions of users had stopped using such applications, suggesting that some readers were turned off by frictionless sharing; nonetheless, some readers suggest that the drop-off is merely because of Facebook altering how shared articles were displayed on a reader's Facebook page (Purewal 2012). The threat of social reading to intellectual privacy is thus likely to persist in the future.

III. THREATS AND PUBLIC POLICY CONSIDERATIONS

A. Government Threats and Impacts on Intellectual Freedom and Privacy

1. National Security

Throughout history, governments have interfered with an individual's intellectual freedom and privacy in the name of national security. As noted earlier, such efforts by the British Crown during the colonial period resulted in the protections of

persons, houses, and papers in the text of the Fourth Amendment. More recently, during the McCarthy era in the 1950s, the United States government used library records to uncover suspected communists and other political dissidents (Martin 2003). In the 1970s, government officials sought reader records on political radicals and anti-Vietnam activists; and in the 1980s the Federal Bureau of Investigation (FBI) sought circulation records for "suspicious looking foreigners" through a Library Awareness Program (ALA 2012c). A Freedom of Information Act (FOIA) Request in 1989 revealed that 266 critics of the Library Awareness Program were subjected to FBI index checks (ALA 2012c). Local law enforcement has also attempted, albeit unsuccessfully, to use library records for fishing expeditions to build evidence for a criminal prosecution (ALA 2012c).

2. USA PATRIOT Act Section 215

The most recent government action in this sphere is Section 215 of the USA PATRIOT Act, which authorized the government to obtain "any tangible thing," including confidential library reader records, book sale records, and book customer lists for a national security investigation (USA PATRIOT Act of 2001, § 215). Proponents of the act argued that opening up library and book

records was critical to national security, so that law enforcement agents could have access to more information, enhancing their ability to uncover terrorist plots (Martin 2003). Section 212 of the Act also authorized librarians to pass over any information to a government entity if the librarian, "in good faith, believes that an emergency involving danger or death or serious physical injury to any person requires disclosure" (USA PATRIOT Act of 2001, § 212).

Pursuant to Section 215, a federal agent can apply to a federal District Court or magistrate judge to obtain library records providing "a statement of facts showing that there are reasonable grounds to believe that tangible things sought are relevant to an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities" (50 U.S.C.A. § 1861(a)(1); West 2012). This standard is lower than a probable cause standard and does not require the government to provide specific, articulable facts that there is a reasonable belief that these records will assist with an authorized investigation (Martin 2003; Woods 2005). These orders are also subject to a gag order, mandating that the recipient of an order

cannot reveal the order, so that the content of the FBI application remains secret. The Act also specifically states that the FBI is not authorized to obtain records on US citizens who are carrying out "activities protected by the first amendment of the Constitution" (50 U.S.C.A. § 1861(a)(1); West 2012).

The ALA and other privacy and intellectual freedom advocates severely criticized Section 215 for having a chilling effect on First Amendment liberties and violating Fourth Amendment rights by lowering the standard required to obtain the records (Martin 2003; ALA 2009). In response to some of this criticism, Section 215 was amended to allow for enhanced oversight in 2006. (USA Patriot Act 2006). This amendment provides a librarian with the right to consult with an attorney about a PATRIOT Act order and required the Attorney General to inform and submit reports about all of the requests under Section 215 to the U.S. House of Representatives' Permanent Select Committee of Intelligence of the House and the U.S. Senate's Select Committee on Intelligence and Committee on the Judiciary in April of every year. (50 U.S.C.A. § 1862 (West)).

Nonetheless, the ALA and privacy and intellectual freedom advocates argue that the enhanced oversight amendment does not

go far enough. The ALA recently launched a campaign to address the USA PATRIOT Act's intrusions into reader privacy (ALA 2012a). This campaign advocates for restoring reader privacy prior to the PATRIOT Act by allowing the Act to sunset (ALA 2012a).

In 2007, the Office of Inspector General (OIG) in the Department of Justice (DOJ) conducted an assessment of Section 215 and discovered the following:

- The first Section 215 request was not made until May 2004
- From May 2004- 2005, 21 solely Section 215 orders were obtained and 141 Section 215 orders were obtained in combination with a pen register or wiretap order
- All 162 of these requests were approved by the Foreign Intelligence Surveillance Act Court and only four were slightly modified from the original request by the Court
- Two of these Section 215 orders were improperly requested
- There was no evidence that information obtained from these orders helped uncover a terrorist plot
- None of these orders were used to obtain library records (US Department of Justice 2007)

The USA PATRIOT Act has been reauthorized several times, the last in May 26, 2011 when President Obama signed S. 990 the "Patriot Sunsets Extension Act of 2011," extending certain

surveillance provisions, including Section 215, for four years (White House 2011). While the latest DOJ OIG report from 2012 mentions that the Office is reviewing Section 215 applications filed between 2007 to 2009, there is no information provided on whether there has been any improper or illegal uses of this Section (US Department of Justice 2012, 16-17).

3. Cybersecurity Programs

In addition to Section 215, the National Security Agency (NSA) and the Department of Homeland Security (DHS) have invested billions of dollars in cybersecurity and have discussed launching such cybersecurity programs as "Perfect Citizen" and "EINSTEIN," some of which may include electronic surveillance of users on the Internet. (Adhikar 2012; Nojem 2012). As recently as February 2012, DHS was under congressional scrutiny when news media reported that the government monitors social networking activity and the postings of comments on online newspapers sites (Stone 2012). DHS maintained that these actions are not intended to curb online speech, but rather capture "situational awareness" during breaking news events and natural disasters (Stone 2012).

Gregory Nojeim suggests that there should be more transparency in how cybersecurity programs protect civil liberties

and that the National Security Agency, the lead agency in this area, may not be the most appropriate agency to safeguard civil liberties (Nojeim 2010).

4. Government Action in the Private Sector

Government action has also affected the private sector's privacy and confidentiality policies. In 2006 in an action concerning COPA, the Child Online Protection Act, the U.S. Department of Justice filed a court order seeking a random sample of 50,000 URLs and 5,000 user search queries from Google's online search engine database over a one-week period without seeking any personally identifiable information to the user's identity[3] (Gonzales 2006). Many leading search engines apparently handed the information over without protest, but Google challenged the subpoena, stating that their user policy assured users of their privacy and anonymity (Gonzales 2006). Google won a partial victory. The Court held that Google had to produce a random selection of 50,000 URLs from Google's database as long as proprietary information was not compromised, but that it did not need to disclose user search terms as the DOJ did

[3] The Child Online Protection Act (COPA) was struck down in 2007.

not meet its burden under discovery standards (Gonzales 2006). While the Court did not make an express ruling on privacy, it did recognize that considerable privacy issues are raised when discussing a user's search data (Gonzales 2006).

Some private online companies like Facebook, Twitter, and Google play a unique role in society as networking tools that connect millions of users to each other. On these networking sites or search engines, users may consider that their activity is limited or private, but in reality this information may be shared with third parties and used to provide targeted advertisements (Ghitis 2012). To what extent actions on Facebook or Google are private or can be shared with the government is still an open issue and is hotly debated. As these companies have access to millions of users' information, habits, and opinions, it should be no surprise that the government is keenly interested in this data. At the time of writing, the government is interested in obtaining cyber threat information from online web companies. The Cyber Intelligence Sharing Protection Act (CISPA) was passed by the House in April 2012 and authorizes companies to share vital information on cyber threats with the government (Tsukayama 2012). President Obama states that he would veto the bill in its current form, citing privacy

concerns (Tsukayama 2012). Privacy advocates are concerned that this cybersecurity mission will be a mechanism for the government to obtain all kinds of personally identifiable information and private user data and that the government will use this data for national security, outside of cyber threats (Tsukayama 2012).

5. Emerging Technologies and the Free Flow of Information

Emerging technologies can have a dual effect on intellectual access and privacy. Instead of inhibiting the right to know, such technologies can also enhance individuals' access to information. New technologies, including web-based applications that share articles and books within a person's network, promote an open and collaborative learning environment (Zu 2009). Therefore, patrons may prefer relaxed privacy policies (Zu 2009).

The free flow of information can be valuable to both businesses and consumers. Fred H. Cate emphasizes the importance of a balanced approach to privacy on the Internet and that too much regulation in the private sector can interfere with information flows (Cate 2000). Protecting an individual's privacy

can create high transaction costs, resulting in inaccurate and incomplete information (Cate 2000). Technology companies such as Facebook and academics like Journalism Professor Jeff Jarvis have also advocated for the values of sharing (Jarvis 2011).

Julie Cohen notes, however, that copyright management technologies are used to monitor readers' habits once they access reading materials, so that owners of this information can prevent widespread infringement; however, she stresses that these technologies can "entail total loss of reader anonymity in cyberspace" (Cohen 1996). Therefore, she urges for Congress to adopt copyright laws that protect readers against anonymity-destroying practices (Cohen 1996).

While technologies continue to advance and develop, breaking down more barriers to reader data, Richards recommends that policymakers keep in mind four principles: 1) reader data is sensitive and may cause harm if wrongly disclosed; 2) readers require real notice on data collecting practices so they can behave accordingly; 3) readers must be provided with a real conscious choice to share information instead of frictionless sharing; and 4) confidentiality rules can be a best practice for ensuring information is properly shared without invading intellectual privacy. Adherence

to these principles, he argues, could allow us to obtain some of the benefits of new digital technologies without sacrificing our intellectual privacy (Richards 2013).

References

Adhikari, Richard. 2010. "Report: NSA Heads Up 'Perfect' Plan to Hunt Down Cyberthreats, TechNewsWorld, (Jul. 18, 2010), http://www.technewsworld.com/rsstory/70374.html.

American Library Association (ALA). 2002 Privacy: An Interpretation of the Library Bill of Rights, Jun. 19, 2002, http://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/intfreedom/librarybill/interpretations/privacyinterpretation.pdf.

American Library Association (ALA). 2009. Resolution on the Reauthorization of Section 215 of the USA PATRIOT ACT, 2009, http://www.ala.org/offices/oif/ifissues/2009usapatriotactreauthorize (last visited Jun. 13, 2012).

American Library Association (ALA). 2012a. Campaign for Reader Privacy, www.readerprivacy.org (last visited Jun. 13, 2012).

American Library Association (ALA). 2012b. Code of Ethics of American Library Association, http://www.ala.org/advocacy/proethics/codeofethics/codeethics (last visited Jun. 13, 2012).

American Library Association (ALA). 2012c. American Library Association Office for Intellectual Freedom, Intellectual Freedom Manual, (8th ed. 2012).

Blitz, Marc Jonathan. 2006. Constitutional Safeguards for Silent Experiments in Living: Libraries, the Right to Read, and A First Amendment Theory for an Unaccompanied Right to Receive Information, 74 UMKC L. Rev. 799, 805.

CAL. CIV. CODE § 1799.3 (2012).

Cate, Fred H. 2000. Principles of Internet Privacy, 32 Conn. L. Rev. 877.

Cohen, Julie E. 2012. Configuring the Networked Self: Law, Code, and the Play of Everyday Practice.

Cohen, Julie E. 2003. Drm and Privacy, 18 Berkeley Tech. L.J. 575 (2003).

Cohen, Julie E. 1996. A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace, 28 Conn. L. Rev. 981.

Emerson, Thomas. 1976. Legal Foundations for the Right to Know, 1976 Wash. Univ. L.Q. 1.

Ghitis, Frida. 2012. Google Know Too Much about You, CNN, (Feb. 9, 2012), http://www.cnn.com/2012/02/09/opinion/ghitis-google-privacy/index.html.

Gonzales v. Google, Inc., 234 F.R.D. 674 (N.D. Cal. 2006).

Jarvis, Jeff. 2011. Public Parts: How Sharing in the Digital Age Improves the Way We Work and Live. Place?: Simon & Schuster.

Katz v. United States, 389 U.S. 347 (1967).

Klinefelter, Ann, http://www.ncjolt.org/sites/default/files/Klinefelter_Anne_v11i3_553_563.pdf, correct cite needs to be added.Martin, Kathryn. 2003. The USA Patriot Act's Application to Library Patron Records, 29 J. Legis. 283.

The Library Company. 2012. At the Instance of Benjamin Franklin: A Brief History of The Library Company of Philadelphia, The Library Company, http://www.librarycompany.org/about/Instance.pdf (last visited Jul. 16, 2012).

MICH. COMP. LAWS § 445.1712 (1988).

Morse, John T. 1989. Benjamin Franklin (1st ed. 1898).

Nissenbaum, Helen. 2010. Privacy in Context: Technology, Policy and the Integrity of Social Life.

Nissenbaum, Helen. 2004. Privacy As Contextual Integrity, 79 Wash. L. Rev. 119.

Nojeim, Gregory T. 2010. Cybersecurity and Freedom on the Internet, 4 J. Nat'l Security L. & Pol'y 119.

Olmstead v. United States, 277 U.S. 438 (1928).

Purewal, Sarah Jacobsson. 2012. Facebook Social Reader Users are Fleeing in Droves, PCWorld, (May 8), http://www.pcworld.com/article/255210/facebooks_social_reader_users_are_fleeing_in_droves.html .

Richards, Neil M. 2013a, The Dangers of Surveillance, 126 Harv. L. Rev. 1934.

Richards, Neil M. 2013b. The Perils of Social Reading, 101 Geo. L. J. 689.

Richards, Neil M. 2011. Limits of Tort Privacy, 9 J. Telecom. & High Tech. L. 357.

Richards, Neil M. 2010. The Puzzle of Brandeis, Privacy and Speech, 63 Vand. L. Rev. 1295.

Richards, Neil M. 2008. Intellectual Privacy, 87 Tex. L. Rev. 387.

Richards, Neil M. 2005. Reconciling Data Privacy and the First Amendment, 52 UCLA L. Rev. 1149.

Richards, Neil M., and Daniel J. Solove. 2010. Prosser's Privacy Law: A Mixed Legacy, 98 Calif. L. Rev. 1887.

Snyder v. Phelps, 131 S. Ct. 1207 (2011).

Solove, Daniel J. 2010. Understanding Privacy.

Solove, Daniel J. 2007. The First Amendment As Criminal Procedure, 82 N.Y.U. L. Rev. 112.

Solove, Daniel J. and Neil M. Richards. 2009. Rethinking Free Speech and Civil Liability, 109 Colum. L. Rev. 1650.

Solove, Daniel J., and Paul M. Schwarz. 2011. Information Privacy Law, (4th ed. 2011).

Stanley v. Georgia, 394 U.S. 557 (1969).

Stone, Andrea. 2012. DHS Monitoring Of Social Media Under Scrutiny By Lawmakers, Huffingtonpost.com, (Feb. 16), http://www.huffingtonpost.com/2012/02/16/dhs-monitoring-of-social-media_n_1282494.html.

Stuntz, William J. 1995. The Substantive Origins of Criminal Procedure, 105 Yale L.J. 393,

395.

Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044 (Colo. 2002).

Tsukayama, Hayley. 2012. CISPA: Who's for it, who's against it and how it could affect you, Wash. Post, (Apr. 27, 2012), http://www.washingtonpost.com/business/technology/cispa-whos-for-it-whos-against-it-and-how-it-could-affect-you/2012/04/27/gIQA5urolT_story.html.

United States v. Am. Library Ass'n, Inc., 539 U.S. 194 (2003).

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot) Act of 2001 § 215, 50 U.S.C.A. §§ 1861-1862 (West Supp. 2002).

USA Patriot and Improvement Act of 2005, PL 109–177, March 9, 2006, 120 Stat 192.

U.S. Department of Justice. 2007. Office of Inspector General, A Review of the Federal Bureau of Investigation's Use of Section 215 Orders for Business Records, Mar. 2007, http://www.justice.gov/oig/special/s0703a/final.pdf.

U.S. Department of Justice. 2012. Office of Inspector General, Report to Congress on Implementation of Section 1001 of the USA PATRIOT Act, Feb, http://www.justice.gov/oig/special/2012/s1202.pdf.

Warren, Samuel D., and Louis D. Brandeis. 1890. The Right to Privacy, 4 Harv. L. Rev. 193.

Westin, Alan. 1967. Privacy and Freedom (1967).

White House. Press Release, Statement by the Press Secretary on S. 990, Whitehouse.gov, May 26. 2011, http://www.whitehouse.gov/the-press-office/2011/05/26/statement-press-secretary-s-990.

Whitney v. California, 274 U.S. 357. (1927)

Woods, Michael J. 2005. Counterintelligence and Access to Transactional Records: A Practical History of Usa Patriot Act Section 215, 1 J. Nat'l Security L. & Pol'y 37.

Zu, Chen, et. al. 2009. The Academic Library Meets Web 2.0- Applications and Implications, 35 J. Acad. Librarianship 324. http://eprints.rclis.org/bitstream/10760/10750/1/The_Academic_Library_Meets_Web_2.0-_Applications_%26_Implications.pdf.