Pro Se Patrons in the Law Library:
The Case for Privacy in the Digital Age

Christine Ford

Submitted to
Professor Richard Jost
Current Issues in Law Librarianship, LIS 595
Law Librarianship, MLIS
University of Washington Information School
May 23, 2017

Abstract:
Maintaining privacy and confidentiality of library patron records is especially difficult in a digital world, but is increasingly critical given the large amount of information that is and can be collected. Privacy is especially important in a law library with respect to pro se patrons because they are entitled to two layers of protection: general library protections (statutorily and ethically) and a work product privilege protection for those who are either actively in or in anticipation of litigation. In this digital era, libraries are not taking a holistic view of records and need to be mindful of how personal information is stored on computers and can be vulnerable to hacking. Law librarians should reexamine and revise their policies and practices to better affirm the values of the profession and provide an improved, more confidential service to patrons.

Table of Contents

"Arguing that you don't care about privacy because you have nothing to hide is like arguing that you don't care about free speech because you have nothing to say."
-Edward Snowden[1]

I. Introduction

Libraries embody and protect many deeply held American and democratic values and, as such, deserve respect and protection from censorship, surveillance, and intrusion. Law libraries provide access to legal information, a crucial service for citizens exercising their rights of self-representation. Despite a broad consensus among professional librarians, representatives in government, and the American populace that libraries should be sacred spaces where one can feel free to pursue whatever informational and intellectual pursuit they wish, law enforcement agencies have regularly requested that librarians monitor and disclose information about their patrons' library usage. Law librarians are tasked with preserving the confidentiality of their patrons; first simply because they are librarians and have an ethical duty to do so, but additionally because public patrons representing themselves in court should be afforded the same right as an attorney to do research on their case and the governing law without fear of discovery of their "work product." In the modern digital era, this requires a close look at how librarians store information, intentionally or otherwise, the ongoing development of policies to maintain privacy, and a continual mindfulness that librarians are the guardians of a wealth of personal information that can be damaging if revealed.

[1] Paul Schrodt, *Edward Snowden Just Made an Impassioned Argument for Why Privacy is the Most Important Right,* Bus. Insider (Sept. 15, 2016), http://www.businessinsider.com/edward-snowden-privacy-argument-2016-9.

II. The History of the Right to Privacy

The Supreme Court has long recognized an implicit right to privacy in the Bill of Rights. The idea of a Constitutional right to privacy was specifically elucidated in *Griswold v. Connecticut* (1965)[2]. The Court determined that there are "penumbras" created by "emanations of guarantees" in the Bill of Rights that elude to a "zone of privacy." Specifically, Justice Douglas, who wrote the majority opinion in *Griswold*, notes that the "spirit" of privacy can be seen in the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments.[3] *Griswold* was referring to marital privacy in the context of family planning and healthcare decisions, but the guarantee of privacy has extended to many other spheres in the more than 50 years since the decision.[4]

Libraries have also long recognized the need for privacy, specifically the necessity of patron records privacy. The American Library Association ("ALA") in its "Privacy: An Interpretation of the Library Bill of Rights" states that privacy is "implicit in the Library Bill of Rights" in that privacy is "essential to the exercise of free speech, free thought, and free association."[5] This interpretation of the Library Bill of Rights goes on to say that the organization "affirms the ethical imperative to provide unrestricted access to information and to guard against the impediments to open inquiry... Lack of privacy and confidentiality has a chilling effect on users' choices. All users have a right to be free from any unreasonable intrusion into or surveillance of their lawful library use." The ALA says that it first disseminated

---

[2] *Griswold v. Connecticut*, 381 U.S. 479 (1965).
[3] *Id.*
[4] *Id.*
[5] ALA, *Privacy: An Interpretation of the Library Bill of Rights*, http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy (last updated July 1, 2014).

the policy of privacy in 1939 in article 11 of its Code of Ethics for librarians: "it is the librarian's obligation to treat as confidential any private information obtained through contact with library patrons."[6] Now it asserts that, "the library profession has a long-standing commitment to an ethic of facilitating, not monitoring, access to information."[7]

History of Government Surveillance of/Requests for Library Records

Policies about privacy and confidentiality in libraries are in place primarily to prevent their disclosure to actors outside of the library, especially the government. This concern has been repeatedly legitimized by laws, programs, and agency policies that attempt to identify political dissidents through library usage and activities. Historically librarians have been at the forefront of the fight for privacy and resistance against government surveillance. The ALA says that it "regularly receives reports of visits by agents of federal, state, and local law enforcement agencies to libraries, asking for personally identifiable information about library users."[8]

In the post-World War II era of McCarthyism, government investigators sought to use library records to identify communists.[9] In June 1953, the ALA responded with the "Freedom to Read Statement" which states, "It is the responsibility of publishers and librarians, as guardians of the people's freedom to read, to contest encroachments upon that freedom by individuals or

---

[6] ALA, *History of the Code of Ethics: 1939 Code of Ethics for Librarians*, http://www.ala.org/Template.cfm?Section=History1&Template=/ContentManagement/ContentDisplay.cfm&ContentID=8875 (accessed May 21, 2017).
[7] *Privacy: An Interpretation of the Library Bill of Rights, supra* n. 3.
[8] ALA, *Policy Concerning Confidentiality of Personally Identifiable Information about Library Users,* http://www.ala.org/advocacy/intfreedom/statementspols/otherpolicies/policyconcerning
[9] http://www.nytimes.com/2001/04/08/weekinreview/ideas-trends-using-books-as-evidence-against-their-readers.html (last updated June 30, 2004).

groups seeking to impose their own standards or tastes upon the community at large; and by the government whenever it seeks to reduce or deny public access to public information."[10]

During the Vietnam War, the government sought to use library records and even librarian testimony to identify citizens with politically opposing viewpoints. Zoia Horn, a librarian and head of the Reference Department at Bucknell University, was subpoenaed in 1972 to testify about the relationships she had developed with specific library patrons, known as the Harrisburg Seven, who were active in the anti-war movement and were accused of conspiring to raid federal offices, bomb government property, and kidnap presidential aide and national security advisor Henry Kissinger.[11] After consulting with an attorney, Horn refused to testify and was held in jail for civil contempt of court for the duration of the trial, in total about twenty days.[12] She was, as

---

[10] ALA, *The Freedom to Read Statement,* http://www.ala.org/advocacy/intfreedom/statementspols/freedomreadstatement (last updated June 30, 2004).

[11] Zoia Horn, *Zoia! Memoirs of Zoia Horn, Battler for the People's Right to Know* (McFarland & Co. 1995); Bob Egelko, *Zoia Horn, Librarian Jailed for Not Testifying Against Protestors*, S.F. Gate (July 15, 2014), http://www.sfgate.com/nation/article/Zoia-Horn-1st-U-S-librarian-jailed-over-alleged-5624023.php; Sarah Lamdan, *Library Patron Privacy in 2014—Honoring the Legacy of Zoia Horn,* CUNY Academic Works (2014), http://academicworks.cuny.edu/cl_pubs/58.

[12] Horn, *supra* n. 9, at 147 (the below written statement by Zoia Horn to the judge); William O'Rourke, *The Harrisburg 7 and the New Catholic Left* (Crowell 1972) xiii (The Seven were a group of anti-war, anti-draft activists, six of whom were Roman Catholic clergy members. They were accused of conspiring to raid federal offices, bomb government property, and kidnap presidential aide and national security advisor Henry Kissinger. In the wake of the police shooting of students at Kent University and the growing anti-war movement on Bucknell's campus, Zoia was understandably unsettled when two FBI agents unexpectedly arrived at her home to ask questions and refused to tell her what it was regarding. She declined to answer questions and was subsequently subpoenaed to a federal grand jury, where she learned that the charges were for conspiracy against a group of library patrons, some of whom she had met briefly, once or twice, in a social context and as a member of the antiwar movement; she answered questions about the social gatherings. Also called to testify at the grand jury was Sister Jogues who, on the advice of counsel, refused to answer questions, claiming that it would compromise the confidentiality of the people she served in her religious capacity. She was held in contempt of court and jailed for four days; Zoia was inspired by Sister Jogues and analogized the confidential nature of the services provided by priests and doctors with that of librarians.

Judith Krug of the ALA's Office for Intellectual Freedom said, "the first librarian who spent time in jail for a value of our profession."[13]

Not all libraries and librarians have gone to such lengths to defend their right to keep patron records private. For example, in 1970 U.S. Treasury agents in Milwaukee and Atlanta requested the records for specific books on explosives.[14] At the direction of the city attorney, the Milwaukee libraries turned over the records, while in Atlanta the libraries declined to comply because the request was not supported by a court order.[15] A subpoena made the difference for the Seattle Public Library in 1974, which compelled the production of 1970 records regarding a forgery case.[16]

Despite having little information, certainly nothing incriminating, Zoia made the decision to refuse to testify at the trial, saying in a written statement to the judge,

> "Your Honor-
>
> It is because I respect the function of this court to protect the rights of the individual, that I must refuse to testify.
>
> I cannot in my conscience lend myself to this black charade. I love and respect this country too much to see a farce made of the tenets upon which it stands.
>
> To me it stands on
>
> *Freedom of thought*—but government spying in homes, in libraries and universities inhibits and destroys this freedom.
>
> It stands on *freedom of association*—yet in this case gatherings of friends, picnics, parties have been given sinister implications, and made suspect.
>
> It stands on *freedom of speech*—yet general discussions have been interpreted by the government as advocacies of conspiracies.
>
> The realities of overt killings in Vietnam have been obscured by the unrealities that I have encountered here.
>
> Legally, I was advised to say that the court's decision denying my request for a wiretap hearing should be challenged and the improper procedure issuing the grant of immunity should be questioned. I believe this.")

[13] Egelko, *supra* n. 9.
[14] David Linowes & Michelle Hoyman, *Data Confidentiality, Social Research and the Government*, 30(3) Lib. Trends 489, 495 (Winter 1982).
[15] *Id.*
[16] *Id.*

As early as the 1970's, but certainly during the 1980's, the Federal Bureau of Investigation ("FBI") made a habit of asking librarians about Soviet efforts to obtain both classified and unclassified information.[17] This policy came to be known as the "Library Awareness Program," and was described as an "educational program designed to inform librarians of the national security threat present in their workplaces."[18] However, they never conducted any educational or training sessions, and librarians reported that it always appeared to be an investigative effort no different from times when the FBI was following specific leads.[19] According to the Deputy Assistant Director of the New York FBI office James Fox, "Hostile intelligence has had some success working the campuses and libraries, and we're just going around telling people what to be alert for. All we are interested in is the fact that a hostile diplomat is there. We don't want librarians to become amateur sleuths."[20] In 1988 the House judiciary subcommittee heard testimony about the Library Awareness Program.[21] Chair of the Committee Rep. Edwards opened with a statement outlining the important missions of both the FBI and libraries, "The subcommittee is well aware that in the foreign counterintelligence area the FBI has awesome responsibilities and for that reason the Congress has given the FBI awesome resources and authorities. But we have not given them unlimited powers and we

---

[17] Ulrika E. Ault, *The FBI's Library Awareness Program: Is Big Brother Reading over Your Shoulder?*, 65 N.Y.U. L. Rev. 1532 (1990).
[18] *Id.* at 1536.
[19] *Id.*
[20] Robert D. McFadden, *F.B.I. in New York Asks Librarians' Aid in Reporting on Spies,* N.Y. Times (Sept. 18, 1987), http://www.nytimes.com/1987/09/18/nyregion/fbi-in-new-york-asks-librarians-aid-in-reporting-on-spies.html.
[21] H. Jud. Subcomm. on Civ. and Const. Rights, *FBI Library Awareness Program: The subcommittee heard testimony on the Federal Bureau of Investigation's Library Awareness Program, a plan to surveil scientific libraries' patrons to try and detect domestic espionage*, TV Broad. (C-SPAN June 20, 1988) (available at https://www.c-span.org/video/?3074-1/fbi-library-awareness-program).

certainly have not authorized them to gain access to information on library usage. Libraries are unique institutions in our society. They are intended to be havens for scholarly work and quiet relaxation. They provide a place for study, reflection, solitude, and intellectual exploration…Library circulation and usage records are not ordinary third party records like telephone toll records or bank records that should be available to intelligence agencies just for the asking."[22] At the time of the hearings 38 states had laws protecting the confidentiality of library records.[23] In the wake of the hearings the remaining states strengthened their protections of library records; today 48 states and the District of Columbia have statutes on the privacy of library records, and the two remaining states, Kentucky and Hawaii, have attorney general's opinions protecting the same right.[24]

III. Privacy Concerns in a Digital Era

With the proliferation of the Internet, personal computers, and mobile devices, privacy has become a frequent and important topic of discussion from a political and legal standpoint. These devices create and store a wealth of personal information that can be exploited for commercial purposes, manipulated by nefarious actors to destroy social and financial reputations, and even have implications in legal proceedings.

Collected digital information can include precise geolocation, financial information, health information, Social Security Numbers, web browsing history, application usage history, and the content of electronic communications. This information can be tracked and stored by

---

[22] *Id.*
[23] Linda Greenhouse, *F.B.I. Search for Spies in Libraries is* Assailed, N.Y. Times (June 21, 1988), http://www.nytimes.com/1988/06/21/us/fbi-search-for-spies-in-libraries-is-assailed.html.
[24] ALA, *State Privacy Laws Regarding Library Records,* http://www.ala.org/advocacy/privacy/statelaws (accessed May 21, 2017).

many different entities, often simultaneously, including websites, third party advertisers, website affiliates, data resellers, Internet service providers, government, and bad actors.[25] Despite concerns about privacy, it is almost impossible to live without using the Internet in today's first world societies.[26]

Commercial Tracking and Data Collection

Not all tracking is nefarious. Data is used in advertising, and it is a lucrative industry.[27] In 2016 alone Internet advertising revenues in the United States totaled $72.5 billion, an increase of 21.8% over 2015.[28] Dr. Alma Whitten, the Privacy Engineering Lead at Google, Inc. testifying before the Senate Committee on Commerce, Science, and Transportation in their Hearing on Consumer Online Privacy, said, "At Google, privacy is something we think about every day across every level of our company. We make this effort because privacy is both good for our users and critical for our business."[29] Whitten emphasizes the fact that Google is free to the user

[25] Anne Klinefelter, *When to Research is to Reveal: The Growing Threat to Attorney and Client Confidentiality from Online Tracking*, 16 Va. J. L. Tech 1 (2011).
[26] Pew Research Center, *Most Working Americans Now Use the Internet or Email at Their Jobs*, (Sept. 24, 2008), http://www.pewinternet.org/2008/09/24/most-working-americans-now-use-the-internet-or-email-at-their-jobs/ (In 2008, Pew reported that 96% of Americans who work use the Internet in their daily lives and 62% use the Internet or e-mail at work); The Department of Commerce Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: Dynamic Policy Framework*, 14 (available at https://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf) ("By 2018, IT employment is expected to grow by another 22 percent").
[27] PricewaterhouseCoopers (PWC), *IAB Internet Advertising Revenue Report 2016 Full Year Results, Interactive Advertising Bureau* (Apr. 26, 2017) (available at https://www.iab.com/wp-content/uploads/2016/04/IAB_Internet_Advertising_Revenue_Report_FY_2016.pdf).
[28] *Id.* at 2.
[29] Alma Whitten, *Testimony of Dr. Alma Whitten, Privacy Engineer Lead, Google Inc.,* Sen. Comm. on Commerce, Science, and Transp., 2 (July 27, 2010) (available at https://static.googleusercontent.com/media/www.google.com/en//googleblogs/pdfs/google_testimony_alma_whitten.pdf).

and they rely on advertisers to continue this model.[30] However, advertising has evolved greatly over time, and now relies on data to show users products and services that are specifically tailored to them, a practice known as behavioral advertising, or Internet-based advertising.[31]

Targeted advertising is so ubiquitous, modern consumers have come to expect it. For example, Google also uses location information available through mobile devices to determine whether a Google search resulted in a store visit.[32] Famously, Target once used data to identify and target women for advertisement who were pregnant before they had announced it publicly.[33] Amazon created "anticipatory shipping," an idea they patented in 2014.[34] They use data like order history, product search history, and shopping cart activities to predict what customers will buy and when and it begins shipping the product to the nearest "hub" before the customer submits the order online.[35] Even banks can track when their customers are looking for new cars and to pre-approve them for financing.[36]

Saying that they use data for more than commercial advertising, Google points to specific examples like a small business owner who has had success using Google to advertise on the same playing field as a big company, economic value created in Texas for advertisers and online

---

[30] *Id.* at 1.
[31] Simson Garfinkel, *How to Stop the Snoopers: Getting Advertisers to Quit Tracking You May Be Harder Than You Think,* MIT Tech. Rev. (Feb. 22, 2011), https://www.technologyreview.com/s/422858/how-to-stop-the-snoopers/; *supra* n. 27.
[32] Sunil Erevelles, Nobuyuki Fukawa & Linda Swayne, *Big Data Consumer Analytics and the Transformation of Marketing*, 69 J. of Bus. Research 897, 901 (2016).
[33] Chares Duhigg, *How Companies Learn Your Secrets*, N.Y. Times Magazine (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.
[34] *Id.*
[35] *Id.*
[36] In early 2016, I started casually looking for a new car online, and around the same time I called my bank to discuss an entirely separate matter, but the representative on the phone said, "We have a note here that you might be looking to purchase a new care. Would you like to discuss financing options?"

publishers, and advertising for non-profit groups like the American Heart Association and the Susan G. Komen Breast Cancer Foundation.[37]

Malicious Tracking and Data Collection

Tracking and targeted advertising can have negative consequences, both when the data is used intentionally for malicious purposes and unintentional triggering. One 17-year-old girl told a reporter that she wishes to lose 15 pounds and has done some online research on weight loss, but now "Every time I go on the Internet. I'm self-conscious about my weight. I try not to think about it…Then the ads make me start thinking about it."[38] Targeted advertising can exacerbate mental health issues like eating disorders, gambling, shopping, and other addictions, and a myriad of other obsessive compulsive behaviors.

Hackers use tracking software to gather information about individuals for a variety of reasons. One of the uses is a practice called "doxing" which is "a means of vigilantism, defined as the overt collection, aggregation and publication of information of a targeted individual (without his/her consent) on the Internet for public consumption, with the intention of causing embarrassment, humiliation and damages, in a way that threatens the victim's privacy and possibly those around the victim (friends, family members etc.)."[39] Neal Horsley, an early "doxer" created a website in 1997 called the "Nuremberg Files" dedicated to publishing abortion providers including personal information like their home addresses, phone numbers, and

---

[37] *Supra* n. 27 at 1.
[38] Julia Angwin, *The Web's New Gold Mine: Your Secrets—A Journal Investigation Finds That One of the Fastest-Growing Businesses on the Internet is the Business of Spying on Consumers*, Wall St. J. W.1. (July 31, 2010).
[39] Roney S. Mathews, Shaun Aghili & Dale Lindskog, *A Study of Doxing, its Security Implications and Mitigation Strategies for Organization*s (2013), http://infosec.concordia.ab.ca/files/2013/02/Roney_Mathews.pdf.

photographs, and list them as either "working," "wounded," or "fatality."[40] Perhaps the most notable modern doxer group is "Anonymous" which primarily targets reported KKK members.[41] However, their information is not always accurate; they incorrectly identified a Ferguson, Missouri police officer who they claimed had been responsible for shooting black teen Michael Brown, releasing the officer's name and social security number.[42] Needless to say, this can have irreparable consequences.

Police officers are frequently the ones doing the tracking, and it is surprisingly easy for them to conduct mass searches of devices, using packet analyzers on unsecure Wi-Fi networks or IMSI catchers to track the mobile phone activities of nearby users. "IMSI Catchers blend into the mobile network operator's infrastructure impersonating a valid cell tower and therefore attracting nearby phones to register to it."[43] Also called StingRay, law enforcement famously used this technology to amass a large amount of data without a court order, asserting section 215 of the PATRIOT Act as their authority.[44] This use was revealed by Edward Snowden in 2013 and was

---

[40] David S. Cohen & Krysten Connon, *Strikethrough (Fatality): The Origins of Online Stalking of Abortion Providers*, Slate (May 21, 2015), http://www.slate.com/articles/news_and_politics/jurisprudence/2015/05/neal_horsley_of_nuremberg_files_died_true_threats_case_reconsidered_by_supreme.html.

[41] Abby Ohlheiser, *What You Need to Know About Anonymous's Big Anti-KKK Operation*, Wash. Post (Nov. 5, 2015), https://www.washingtonpost.com/news/the-intersect/wp/2015/11/05/what-you-need-to-know-about-anonymouss-big-anti-kkk-operation/?utm_term=.d3b60cd88bec.

[42] *Id.*

[43] Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani & Edgar Weippl, *IMSI-Catch Me If You Can: IMSI-Catcher-Catchers*, Proc. of the Annual Computer Sec. Applications Conf. 246, 247 (2014) (available at http://delivery.acm.org/10.1145/2670000/2664272/p246-dabrowski.pdf?ip=205.175.118.22&id=2664272&acc=ACTIVE%20SERVICE&key=B63ACEF81C6334F5%2EF43F328D6C8418D0%2E4D470,2B0C3E38B35%2E4D4702B0C3E38B35&CFID=764878306&CFTOKEN=39445462&__acm__=1495481510_e3739e94434ff836b762d83da4ab37b0).

[44] Stephanie K. Pel & Chirstopher Sochoian, *A Lot More Than a Pen Register, and Less Than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 Yale J.L. & Tech. 134 (2013-2014).

widely reported in the media, which sparked a congressional inquiry into limiting the National Security Administration's (NSA) investigative powers by offering interpretive guidance on the PATRIOT Act.[45]

The expansion of data and information tracking, along with added security concerns following the 2001 9/11 attacks has made it easy to greatly expand terrorist watch lists like the no-fly list.[46] Then sitting President Obama said during a PBS NewsHour town hall meeting, in response to a question by an audience member about gun control, "I just came from a meeting today in the situation room in which I've got people who we know have been on ISIL websites, living here in the United States, US citizens, and we're allowed to put them on the no-fly list when it comes to airlines, but because of the National Rifle Association, I cannot prohibit those people from buying a gun."[47] While the process by which the government determines an individual should be placed on the no fly list is not public, some examples of the types of people who have been placed on the list raises questions as to the criteria.[48] For example, in 2004 a flight from London to Washington D.C. was diverted to Maine because musician Yusuf Islam, better known by his stage name Cat Stevens, was on board and on the list.[49] Senator Ted Kennedy, in a Senate Judiciary Committee hearing, said that he has been repeatedly stopped and questioned at airports because apparently T. Kennedy is a popular terrorist alias.[50] There are

---

[45] *Id.*; *see also infra* n. 73.
[46] Justin Florence, *Making the No Fly List Fly: A Due Process Model for Terrorist Watchlists*, 115 Yale L.J. 2148, 2153 (2006).
[47] *Obama to Gun Owners—I'm Not Looking to Disarm You*, TV Broad. (PBS June 2, 2016) (available at http://www.pbs.org/newshour/bb/obama-to-gun-owners-im-not-looking-to-disarm-you/).
[48] *Supra* n. 44 at 2155.
[49] Gregory Krieg, *No-Fly Nightmares: The Program's Most Embarrassing Mistakes*, CNN (Dec. 7, 2015), http://www.cnn.com/2015/12/07/politics/no-fly-mistakes-cat-stevens-ted-kennedy-john-lewis/.
[50] *Id.*

numerous tales of small children as young as 9-months-old who are prevented from flying because they have "been flagged as no fly."[51] Once you are on the no fly list, it is very difficult to get off it, even in cases of mistaken identity or clerical error.[52] Governmental tracking of online activity can have real and long-lasting consequences.

Digital Records in Libraries

Also in the "Privacy: An Interpretation of the Library Bill of Rights" is an acknowledgment of the complicating nature of stored digital data on patron records. "Confidentiality extends to, 'information sought or received and resources consulted, borrowed, acquired or transmitted,' including but not limited to: database search records, reference questions and interview, circulation records, interlibrary loan records, information about materials downloaded or placed on 'hold' or 'reserve,' and other personally identifiable information about uses of library materials, programs, facilities, or services."[53] Library patron records are no longer confined to just the books someone checks out, but rather include the multitude of information a patron might disclose while at the library, either to a reference librarian or to a library computer that is collecting that information.

---

[51] *Id.*; Kristie Rieken, *Four-Year-Old Boy Shows up on Government 'No-Fly' List*, Assoc. Press (Jan. 5, 2006) (available at https://news.google.com/newspapers?nid=861&dat=20060106&id=JulYAAAAIBAJ&sjid=rVYMAAAAIBAJ&pg=3945,947845&hl=en); Caroline Drees, *US No-Fly List Vexes Travelers from Babies on up,* Reuters (Dec. 15, 2005) (available at http://www.redorbit.com/news/general/331376/us_nofly_list_vexes_travelers_from_babies_on_up/) ("Sarah Zapolsky was checking in for a flight to Italy when she discovered her 9-month-old son's name was on the United States' "no-fly" list of suspected terrorists.").

[52] *Supra* n. 47.

[53] *Supra* n. 3.

IV. Statutory Regulation

Regarding Digital Privacy

During its development, the Internet was not intended for widespread use, but rather as a research tool to be used in universities and by the government.[54] Recognizing the value and broader applications, technology vendors began incorporating computer networking capabilities into their products as early as the 1980's.[55]

Despite rapidly changing technology, laws regarding digital privacy have remained largely the same. The Electronic Communications Privacy Act of 1986 (ECPA) is still the controlling law on the government's right to access individuals' electronic communications.[56] The ECPA broadly defines electronic communications as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[57] These communications during transfer are subject to a "court order" requirement.[58] Technology has changed such that most communications are never solely in

---

[54] Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts & Stephen Wolff, *A Brief History of the Internet,* 39(5) Computer Commun. Rev. (newsltr. of ACM SIGCOMM) 22, 29 (available at http://delivery.acm.org/10.1145/1630000/1629613/p22-leiner.pdf?ip=128.95.184.210&id=1629613&acc=ACTIVE%20SERVICE&key=B63ACEF81C6334F5%2EF43F328D6C8418D0%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&CFID=936073575&CFTOKEN=77448652&__acm__=1494705186_b35bf6b0cd0dfac73f0c478b56f6c5c2) ("Starting in the early 1980's and continuing to this day, the Internet grew beyond its primarily research roots to include both a broad user community and increased commercial activity.")

[55] *Id.*

[56] Alexandra Vesalga, *Location, Location, Location: Updating the Electronic Communications Privacy Act to Protect Geolocational Data*, 43 Golden Gate U. L. Rev. 459 (Summer 2013); *Hutton v. Woodall*, 70 F. Supp. 3d 1235 (2014) (holding that the ECPA is unconstitutional as applied to non-governmental actors).

[57] 18 U.S.C.A. § 2510(12) (2002).

[58] *Id.* at § 9(b).

transit, but rather stored on third-party servers at minimum in the process of transmission, if not longer.[59] Stored communications are treated differently (under a section of the ECPA called the Stored Communications Act); obtaining the contents of a communication still requires a warrant, but the government can obtain "records concerning electronic communication service" through a variety of channels, including the consent of a subscriber or if it relates to "telemarketer fraud."[60]

The ECPA has almost universally been panned as in desperate need of updating.[61] Even Senator Patrick Leahy of Vermont, who originally drafted the ECPA, and who is still in office today, called for reform of the law.[62] In 2011, on the 25th anniversary of the bill's enactment, Leahy said, "When I led the effort to write the ECPA 25 years ago, no one could have contemplated the many emerging threats to our digital privacy. But, today, this law is significantly outdated and out-paced by rapid changes in technology and the changing mission of our law enforcement agencies after September 11. At a time in our history when American consumers and businesses face threats to privacy like no time before, we must renew the

[59] Vesalga *supra* n. 47 at 470.
[60] 18 U.S.C.A. § 2703(c)(1) (2009).
[61] *Supra* n. 27 at 21 ("Other legal restraints on monitoring online activity include the Electronic Communications Privacy Act and the Stored Communications Act, but these laws were written for older technologies, and their utility in the evolving symbiotic web has been questioned, particularly when the data collector is agreeable to sharing tracking data."); Orin S. Kerr, *A User's Guide to the Stored Communications Act and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208 (2004) (gives the SCA an overall "B" grade, but calls for reform through simplifying, clarifying, and strengthening the law); Alison Macrina, Speech, *Practical Tools to Safeguard Digital Privacy* (Dublin, Ireland Feb. 11, 2016) (given at the annual conference for the Academic & Special Lib. section of Lib. Assoc. of Ir., video recording available at https://www.youtube.com/watch?v=Ezt9ep2j-HE&t=621s) ("The ECPA was passed in 1985 when one gigabyte of data cost $90,000 … Laws were created when no one had any idea how massive this thing [the Internet] would scale, how cheap it would get to be to store information.").
[62] *Leahy Marks 25th Anniversary of ECPA, Announces Plan to Mark up Reform Bill,* https://www.leahy.senate.gov/press/leahy-marks-25th-anniversary-of-ecpa-announces-plan-to-mark-up-reform-bill (Oct. 20, 2011).

commitment to the privacy principles that gave birth to the ECPA a quarter century ago."[63] Senator Leahy introduced the Electronic Communications Privacy Act Amendments Act in 2011 and then again in 2013.[64] It was sent to the Committee on the Judiciary where Senator Leahy submitted a written report, but no further action has been taken.[65]

While several agencies have attempted to regulate online tracking by businesses for advertising purposes, the Federal Trade Commission (FTC) has emerged as the "lead federal agency addressing consumer privacy concerns in the United States.[66] Businesses might not have nefarious intentions when collecting data, but they are a target for hackers, presenting massive security problems.[67] The FTC's mission is to "protect consumers by preventing anticompetitive, deceptive, and unfair business practices, enhancing informed consumer choice and public understanding of the competitive process, and accomplishing this without unduly burdening legitimate business activity."[68] The FTC uses two different, but not mutually exclusive frameworks: the 1990's-era "fair information practice principles," with a focus on notice, choice, access, and security, which requires companies to provide notice of what they wish to collect and allow consumers to choose what information is collected about them and, the more recent, more

---

[63] *Id.*
[64] 113th Congress (2013-2014), *S.607—Electronic Communications Privacy Act Amendments Act of 2013*, https://www.congress.gov/bill/113th-congress/senate-bill/607/actions (accessed May 21, 2017).
[65] *Id.*
[66] *Supra* n. 27 at 21; Maureen Ohlhausen, *Privacy Challenges and Opportunities: The Role of the Federal Trade Commission*, 33 J. of Pub. Policy & Mktg. 4 (Spring 2014).
[67] Chris Isidore, *Target: Hacking hit up to 110 Million Customers*, CNN Money (Jan. 11, 2014), http://money.cnn.com/2014/01/10/news/companies/target-hacking/ ("The breach occurred in the weeks following Thanksgiving when as many as 40 million customers may also had credit or debit card information stolen.").
[68] FTC, *About the FTC: Our Mission*, https://www.ftc.gov/about-ftc (accessed May 21, 2017).

relaxed "harms-based" approach.[69] Saying the notice-and-choice requirements are "potentially costly" because they cover "all uses of information," the FTC calls the harms-based approach "targeted [to] practices that caused or were likely to cause physical or economic harm, or 'unwarranted intrusions in [consumers'] daily lives.'"[70] The FTC has statutory authority to enforce consumer privacy protections, and to take action against "unfair or deceptive acts or practices in or affecting commerce."[71] The FTC has exercised this authority in the context of consumer privacy on a handful of occasions, including against Gateway Learning Corporation (doing business as "Hooked on Phonics") in 2004 for selling private consumer information to third-parties without providing notice, against Facebook in 2012 for a similar practice, and against several rent-to-own companies for installing software on rented computers that collected private information.[72]

The USA PATRIOT Act and Library Patron Records

The USA PATRIOT Act has gotten a lot attention, and has been the subject of much discussion and speculation as to its effect on the privacy of library records.[73] The PATRIOT Act

[69] Ohlhausen *supra* n. 64 at 3; FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress*, 3-4, https://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission (May 2000); FTC, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, Prelim. FTC Staff Rpt. 9, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf (Dec. 2010).
[70] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Id.*
[71] Ohlhausen *supra* n. 64 at 5 (citing Section 5 of the FTC Act, 15 U.S.C. § 45(a)(1) (2006)).
[72] Ohlhausen *supra* n. 64 at 6.
[73] Kathryn Martin, *The USA PATRIOT Act's Application to Library Patron Records*, 29 J. Legis. 283 (2003).

was passed on October 26, 2001 in the wake of the 9/11 attacks, with the purpose "to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes.[74] The operative language used to gather confidential information from libraries is section 215 which gives the Federal Bureau of Investigation the authority to order "the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information…"[75] It specifically says this order can include "library circulation records, library patron lists."[76] Under the statute, the FBI does need to apply for a court order compelling the disclosure, however the standard is greatly relaxed, and does not need to allege any specific facts, only that "a significant purpose" of the disclosure is the investigation of terrorism or foreign intelligence.[77] The orders can come from a court operating under the 1978 Foreign Intelligence Surveillance Act, which prevents libraries and librarians from disclosing the existence of a warrant or that any records were produced as a result of the warrant.[78]

State Privacy Laws Regarding Library Records

Every state and Washington, D.C. has specifically provided for the confidentiality of library records, either by statute or in an Attorney General's Opinion.[79] They vary widely and afford an accordingly wide amount of protection.

---

[74] Pub. L. No. 107–56, 115 Stat 272 (2001).
[75] 50 U.S.C.A. § 1861(a)(1) (2017).
[76] *Id.* at §3.
[77] *Supra* n. 71 at 287.
[78] 50 U.S.C.A. § 1803 (2015); Kings County Library, *Confidentiality of Library Record*s, http://www.kingscountylibrary.org/confidentiality-of-library-records (Nov. 4, 2008).
[79] *Supra* n. 22.

Broadly, almost all of statutes specifically state that they apply to only to public libraries, libraries that receive public funds, or any library that is "open to the public."[80]

What records are covered vary across the statutes, as well. Once again, almost all use language that indicates records that include "personally identifiable information" are confidential and not subject to disclosure.[81] Some states specifically mention circulation and registration records, although many of them point to these as "including but not limited to" coverage.[82] Some states explicitly state that these records can be in print or digital format, and eight of fifty-one explicitly protect "born-digital" or electronic patron data (i.e.: database searches, information collected on library computers, etc.).[83] Three states specifically protect reference "queries" or interactions with reference librarians.[84]

The least comprehensive of the statutes simply include library records in the list of public records that are exempt from Freedom of Information Act disclosures, and approximately eight states do this.[85]

Many include an exception to keeping records confidential in the case of a court order, subpoena or warrant, and some require those orders to include specific findings such as the disclosure is "necessary to protect public safety" or to prosecute a crime. Another common feature of these statutes allows libraries to disclose records to aid in prosecuting a crime committed on library property or to effectively collect lost materials or fines.

---

[80] Appendix A (five states apply broadly to all institutions, including private libraries, that are "open to the public," and Minnesota's applies narrowly only to "government entities").
[81] Appendix A (Alaska's statute states, "personal identifying information of people who have used materials made available to the public by a library").
[82] Appendix A (sixteen states include "circulation" and eight include "registration").
[83] Appendix A.
[84] *Id.*
[85] *Id.*

Notably, some of the statutes will alternately impose liability or prohibit disclosures of protected records or disclaim liability for disclosure under one of the enumerated exceptions.[86] Twelve statutes impose criminal or civil liability for unauthorized disclosure, with maximum punishments of misdemeanor charges including short jail time to fines of $250 plus attorney's fees in civil action.[87]

V. Implications for Law Libraries

Legal research presents its own unique privacy considerations and protections, especially when that research is being done by a lawyer or a party currently involved in litigation. Attorneys and parties (frequently parties representing themselves, called "pro se") use law libraries and law librarians to assist them in better understanding the court system, the law, and how to navigate a complex legal field. The well-established, but somewhat vaguely-defined work-product doctrine protects the research done by these patrons from discovery by an opposing party and from search and seizure by law enforcement.

Work-Product Doctrine

The work-product doctrine has its roots in common law to balance what is intended to be a broad and open discovery process with the absolute privilege and confidentiality inherent in the attorney-client relationship.[88]

---

[86] *Id.*
[87] *Id.*
[88] Jeff A. Anderson, Gina E. Cadieux, George E. Hays & Michael B. Hingerty, *Work Product Doctrine*, 68 Cornell L. Rev. 760, 893 (Aug. 1983).

In 1947, the Supreme Court reinforced the doctrine and offered definitional guidance.[89] "In performing his various duties, however, it is essential that a lawyer work with a certain degree of privacy, free from unnecessary intrusion by opposing parties and their counsel. Proper preparation of a client's case demands that he assemble information, sift what he considers to be the relevant from the irrelevant facts, prepare his legal theories and plan his strategy without undue and needless interference. That is the historical and the necessary way in which lawyers act within the framework of our system of jurisprudence to promote justice and to protect their clients' interests. This work is reflected, of course, in interviews, statements, memoranda, correspondence, briefs, mental impressions, personal beliefs, and countless other tangible and intangible ways—aptly though roughly termed by the Circuit Court of Appeals in this case (153 F.2d 212, 223) as the 'Work product of the lawyer.' Were such materials open to opposing counsel on mere demand, much of what is now put down in writing would remain unwritten. An attorney's thoughts, heretofore inviolate, would not be his own. Inefficiency, unfairness and sharp practices would inevitably develop in the giving of legal advice and in the preparation of cases for trial. The effect on the legal profession would be demoralizing. And the interests of the clients and the cause of justice would be poorly served."[90] The values and rationale behind the work product doctrine, as evident in the *Hickman* decision are (1) preserving the "privacy of preparation" that is essential to the adversarial legal system and (2) the need to protect the "attorney's mental processes."[91]

The 1937 version of the Federal Rules of Civil Procedure (FRCP's) did not mention work-product specifically, but attorneys attempted to limit discovery through rule 30(b) that

[89] *Hickman v. Taylor*, 329 U.S. 495, 510–11 (1947).
[90] *Id*.
[91] *Supra* n. 86 at 785.

stated that a judge could restrict discovery of documents using a protective order on the showing of "good cause."[92] The FRCP's were amended in 1955, and the committee recognized the problems with the "good cause" standard, and early drafts looked to eliminate it, but ultimately the Advisory committee chose to leave it in place, claiming that it did not conflict with the *Hickman* standards.[93] In 1970, with yet more amendments to the FRCP's, the work-product doctrine became much the rule that it is today.[94] The Advisory Committee that drafted the amendments intended to rectify the problems with the "good cause" standard, especially its wildly different treatment and use by judges and also to extend the work-product protection to more people than just attorneys.[95] Rule 26(b)(3) states, "Ordinarily, a party may not discover documents and tangible things that are prepared in anticipation of litigation or for trial by or for another party or its representative (including the other party's attorney, consultant, surety, indemnitor, insurer, or agent)."[96]

The content of what is protected is sometimes referred to in the categories of facts, ordinary work product, opinion work product, and legal theories.[97] Facts, separate from the other types of work product, are discoverable, whereas opinion work product is not.[98] Some courts read the doctrine broadly saying, "The reach of the work product privilege is broad; '[e]ven factual portions of documents may be withheld, so long as the document as a whole was created in anticipation of litigation.'"[99] According to the rule, an opposing party can defeat the privilege

---

[92] *Id.* at 782.
[93] *Id.*
[94] *Id.*
[95] *Id.*
[96] Fed. R. Civ. P. 26.
[97] *Supra* n. 86 at 789.
[98] *Id.*
[99] *Equal Rights Ctr. v. Post Properties, Inc.*, 247 F.R.D. 208, 211 (D.D.C. 2008) (quoting *General Elec. Co. v. Johnson*, No. 00–2855, 2006 WL 2616187, at *12 (D.D.C. Sep.12, 2006).).

if it "shows that it has substantial need for the materials to prepare its case and cannot, without undue hardship, obtain their substantial equivalent by other means.[100]

State procedural codes also typically explicitly guarantee protection under the work product doctrine.[101] Some explicitly mention legal research as privileged. In the criminal context, "All jurisdictions allowing disclosure of witness statements do protect, however, "opinion" work product…Various state discovery rules do not include a work product provision as such. Instead, following the lead of the 1975 version of Federal Rule 16, they have a provision prohibiting discovery of 'reports, memoranda, or other internal government documents made by the attorney for the government or any other government agent investigating or prosecuting the case.' This provision clearly covers all opinion work product and most fact work product as well."[102]

Legal research is almost always considered by courts to be opinion work product, and therefore protected from discovery.[103] A District Court in Washington, D.C. explicitly said, "First, I can find quite easily that legal research by law clerks and attorneys are prepared 'for trial' and reflect the "mental impressions, conclusions, opinions or legal theories of a party's attorney or representative." It is hard to imagine a document that memorializes legal research done by a lawyer or law clerk that is not work product."[104]

---

[100] Fed. R. Civ. P. 26(b)(3)(A).
[101] *Supra* n. 23 at 19-20.
[102] Wayne R. LaFave, Jerold H. Isreal, Nancy J King & Orin S. Kerr, *Criminal Procedure* vol. 5, § 20.3(j) (4th ed., West 2016).
[103] *Soc'y of Prof'l Eng'g Employees in Aerospace, IFPTE Local 2001, AFL-CIO v. Boeing Co.*, 2009 WL 3711599, at *4 (D. Kan. Nov. 3, 2009), adhered to sub nom. *Soc'y of Prof'l Eng'g Employees in Aerospace v. Boeing Co.*, 2010 WL 1141269 (D. Kan. Mar. 22, 2010) (finding that, "Counsels' drafts and legal research during this period are also protected by the attorney work product doctrine.").
[104] *N.L.R.B. v. Jackson Hosp. Corp.*, 257 F.R.D. 302, 310 (D.D.C. 2009).

Much like attorney-client privilege, the protection of work product can be waived, either intentionally or by accident, "by failing to assert the protection, by tendering certain issues, and by conduct inconsistent with claiming the protection."[105] One such action that would preclude subsequently claiming the doctrine is "voluntary disclosure or consent to disclosure of the writing to a person other than the client who has no interest in maintaining the confidentiality of the contents of the writing."[106] This is known as disclosure to a third party, and destroys many types of privileges in many contexts. The Restatement of The Law Governing Lawyers provides further guidance on third party disclosure waiver: "Work-product protection is waived by disclosure to third parties if it occurs in circumstances in which there is a significant likelihood that an adversary in litigation will obtain the materials… Effective trial preparation often entails disclosing work product to coparties and nonparties. Work product, including opinion work product, may generally be disclosed to the client, the client's business advisers or agents, the client's lawyer or other representative, associated lawyers and other professionals working for the client, or persons similarly aligned on a matter of common interest."[107]

The use of computers and other electronic means of communicating and researching complicates the work product doctrine because e-mails, search terms, websites visited, and documents downloaded all involve a third-party server as an intermediary, and, as we have seen, online tracking by third parties is rampant, even of the most diligent online surfers. Despite the possible third-party disclosure, electronic legal research and communication is regularly considered to be opinion work-product by courts. One court's opinion and order state,

---

[105] *McKesson HBOC, Inc. v. Superior Court*, 115 Cal. App. 4th 1229, 1239 (2004).
[106] *Id.* (quoting *BP Alaska Exploration, Inc. v. Superior Court* 199 Cal.App.3d 1240, 1261 (1988).).
[107] *Restatement (Third) of the Law Governing Lawyers* § 91 (2000).

"Defendants assert that five communications are protected by the attorney work product doctrine. Four of these communications contain legal opinions that Near North's General Counsel e-mailed to herself from Lexis–Nexis. The search terms used to gather these cases does provide a window into the attorney's thinking, so these communications would be protected if they were created in anticipation of litigation."[108]

The text of the FRCP's says that it applies to a "party or its representative" although it has been mostly used to protect attorneys in their work on behalf of clients. The issue of who owns the work product privilege has been addressed with regard to whether a lawyer can keep his work product secret from his client, and whether the lawyer or the client has the final say on which documents are produced and when to claim privilege.[109] Both the Federal approach and the Restatement generally side with the client, asserting that shielding documents from the client's view is a perversion of the rationale of *Hickman*.[110] Interpreting the California rule protecting work product, the court in *Dowden v. Superior Court* found that in propria persona [pro se] litigants have a right to assert the privilege.[111] In criminal cases, the argument that a pro se defendant has a right to assert privilege is even stronger.[112] "The work product privilege protects the preparation of lawyers, regardless of the individual lawyer's degree of competence or sophistication, and requires no showing of the quality of the information sought to be protected. There is no viable argument that the pro se defendant's litigation preparation should not be

---

[108] *United States v. Segal*, 2004 WL 830428, at *8 (N.D. Ill. Apr. 16, 2004).
[109] Fred C. Zacharias, *Who Owns Work Product*, 2006 U. Ill. L. Rev. 127 (2006).
[110] *Id.*
[111] *Dowden v. Superior Court*, 86 Cal. Rptr. 2d 180, 185-86 (Ct. App. 1999) ("[the work product privilege] is important not only for attorneys, but also for litigants acting in propria persona. A litigant needs the same opportunity to research relevant law and to prepare his or her case without then having to give that research to an adversary making a discovery request").
[112] J. Vincent Aprile II, *The Pro Se Litigant and the Work Product Privilege*, 31 Crim. Just. 35 (Fall 2016) (quoting *United States v. Nobles*, 422 U.S. 225, 238 (1975).).

covered by the work product privilege because the accused lacks the formal training and experience of a member of the bar."[113] Furthermore, from a public policy, if the courts are going to allow litigants to represent themselves, they need to allow them to do that to the best of their abilities, and encourage thorough research and preparation. Likely a pro se patron has the right to assert work product privilege, both in the civil and criminal context.

VI. Current Library Policies/Practices

Library policies on patron records vary widely, offering a wide variety of language and specific guidance on the keeping of records and the process by which requests for disclosures are handled.

Academic law libraries are the least thorough in their policies about how staff should proceed in the face of a request for disclosure. William and Mary Law School's "Confidentiality of Patron Records" policy simply states "The library abides by all applicable state and federal laws. Unless required by law, the library does not reveal the names of patrons or what items have been checked out."[114] Loyola University Chicago Law School's Library says of patron confidentiality, "The Law Library does not disclose the identity of borrowers or their library records. Please see the Library Confidentiality Act (75 ILCS 70/1) for information regarding Illinois state law and patron confidentiality."[115] Rutgers Law goes a little further saying, "The Law Library respects the rights of patrons to pursue their research and recognizes that the subject of their research is private. Protecting patron privacy and confidentiality is an integral part of the

---

[113] *Id.*
[114] Wolf Law Library, William & Mary Law School, *Confidentiality of Patron Records,* http://law.wm.edu/library/about/policies/confidentiality/index.php (accessed May 21, 2017).
[115] Loyola University Chicago School of Law Library, *Policies: Patron Confidentiality,* http://luc.edu/law/library/about/policies.html#Patron_Confidentiality (accessed May 21, 2017).

mission of the Law Library. In order to ensure this right, the Law Library has adopted the American Library Association Code of Ethics and the New Jersey Confidentiality of Library Records Law, N.J.S.A. 18A: 73-43.1-43.3, as the basis for its privacy policy."[116] These statements may not represent the entirety of their policies, and might not reflect a more extensive, university-wide policy. For example, the University of Washington's Compliance and Risk Services, under the guidance of the University division of the Attorney General's office, has an internal policy for all campus libraries called the "Regulatory Response Guidance: Responding to requests for personal information about faculty, staff and students."[117] The policy has step-by-step instructions on how "Front-line Staff" and supervisors are to handle both in-person requests and requests made by telephone, email or letter.[118] Where possible, a lawyer from the Attorney General's office is consulted to determine what disclosure is legally required, if any at all.[119]

Some public libraries, including public law libraries have much more extensive record policies, like the specific instructions provided by the Attorney General's Office to the University of Washington's libraries. The Public Law Library of King County (PLLKC) in Washington state is a great example of the kind of instructional guidance provided by some policies. "All library records, whose primary purpose is to maintain control of library materials, or to gain access to information, which disclose or could be used to disclose the identity of

---

[116] Rutgers Law School Library, *Library Policies, Using the Law Library, Rules for Patrons, Privacy,* http://library.law.rutgers.edu/library-policies (accessed May 21, 2017).
[117] UW Compliance and Risk Services, *University of Washington Regulatory Response Guidance: Responding to Requests for Personal Information About Faculty, Staff and Students*, https://www.polisci.washington.edu/sites/polisci/files/documents/regulatory_response_guidance_-_responding_to_requests_for_personal_information.pdf (Mar. 22, 2017).
[118] *Id.*
[119] *Id.*

library users are confidential in nature. These include all library circulation records and other records linking the names of library patrons, their addresses and other personal information with specific materials, online sites, and resources they access."[120] The policy goes on to outline "Circumstances, if any under which records will be released" and the procedures by which they are released, including a review by the library's legal counsel of "the service of process, order or subpoena for any legal defect."[121] The Assistant Director of PLLKC elaborated on how they implement these policies in the library, saying that they "(1) rely on automated settings within our ILS to limit the gathering of and access to patron collection use. It divorces user-specific data from circulation activity and only keeps circulation history for individual patrons for a short while… (2) protect patron privacy during the reference interview to the extent possible in an open service desk space but since there is no record created that identifies the patron with the question during these sessions we're comfortable believing we've met privacy concerns. On rare occasions we isolate librarians and patrons away from the primary service desk if there is a heightened sensitivity issue but the downside there is basic safety for the staff so we have to be very careful doing this, (3) deliberately do not include any patron identity data in our statistical instruments, and (4) deliberately do not include any patron identity data in the email statistical measurements we gather."[122] PLLKC also has a Legal Help Center (LHC) staffed by an attorney who can give more concrete legal advice than a reference librarian.[123] Regarding the LHC's

[120] Public Law Library of King County, *Confidentiality of Library Records,* http://pllkc2.org/contact-us/policies/confidentiality-of-library-records/ (last updated Sept. 19, 2012).
[121] *Id.*
[122] Email from Rick Stroup, Asst. Dir. Pub. L. Lib. of King Co. to Christine Ford, *Follow-Up Questions: UW Law Librarianship* (May 11, 2017 11:56 a.m. PDT).
[123] Public Law Library of King County, *Legal Clinics, Rita R. Dermody Legal Help Center,* http://pllkc2.org/legal-clinics/ (accessed May 21, 2017).

records, Stroup said, "The clinic… uses an intake form which our staff attorney reviews to determine if or how the patron can be helped. It lays out explicitly our terms of service regarding legal representation and requires the patron to acknowledge and agree to these terms. Intake forms are destroyed shortly after creation but question and answer statistics are duplicated in an electronic record and will be held indefinitely."[124]

As seen above, written policies do not always reflect the full extent of what a library does to shield its patron records from disclosure, but the more extensive and specific a policy is, the better able its staff are to adhere to it and implement it in an emergent situation.

VII. **Recommendations**

The current laws do not adequately protect individuals and many library policies do not fill in those gaps. Libraries are subject to requests for records not only about materials, but also about reference questions, and the requests come not only from law enforcement officials, but also from private citizens. In 1978, a Kansas journalist requested the library records of city council members.[125] In 1977 another journalist, this time in Washington State requested a local community college library's records.[126] In Illinois a divorced father requested the library's story hour records to prove that his ex-wife had changed his child's name to that of her new husband.[127]

Dr. Alma Whitten, the Privacy Engineering Lead at Google, Inc,., in her Senate Hearing testimony, outlined five privacy principles adhered to by Google: "[1] Use information to

[124] *Supra* n. 120.
[125] Supra n. 12 at 496.
[126] *Id.*
[127] *Id.*

provide our users with valuable products and services, [2] Develop products that reflect strong privacy standards and practices, [3] Make the collection and use of personal information transparent, [4] Give users meaningful choices to protect their privacy, and [5] Be a responsible steward of the information we hold."[128] These principles can broadly be applied to libraries, as well. However, I would caution against the use of "meaningful choice" and "transparency of collection" insomuch as these tools can be likened to "informed consent" in a medical context.

First, we do not yet know what this massive amount of data will mean and how it will be used in the future, because this is the first time in human history that this amount of personal information has been collected. Second, we must acknowledge that laws were made to protect the weakest and most vulnerable of us. The increasing presence of technology in our world has left us almost numb to the omniscience of our devices. Most consumers quickly accept the terms and conditions of every passing website, software program, bill of sale, and more without even glancing at the document. They are more interested in expediency than safety where digital privacy is concerned, and it is not until they are facing a major lawsuit or have had their identity stolen that they realize they consented to the situation, perhaps repeatedly. Most people do not care about privacy until they are among the minority of vulnerable people whose lives have been negatively affected.

Library Policy Recommendations

The most effective library policies on patron records are long, extensive, and outline specific steps that staff should take if presented with a request for patron records. They recommend involving legal counsel as much as is possible, including language that requires

[128] *Supra* n. 27.

attorney review for all civil orders requiring the production of documents, and requesting that counsel be present for any criminal investigations under the authority of a warrant.

A good policy would also outline the library's practices for record creation and retention. First, take stock of all the ways in which library patrons' information is sent and received, where it is stored and for how long. Some considerations:

- E-mail questions to the reference office: How long do deleted e-mails remain in their folder? Is the "sent" folder ever purged?
- Do you support a "chat" function to receive reference questions (i.e. QuestionPoint through OCLC)[129]?
- Where and for how long are e-books and online article download requests stored (i.e. Overdrive through Amazon)?
- What types of information is accessible on your computer terminals? Can sensitive information be stored (i.e. passwords, credit card numbers, etc.)?
- Is your website secure?
- Does the vendor for your integrated library system store information?

[129] OCLC, *QuestionPoint Patron Terms of Service,* https://www.questionpoint.org/ordering/pdfs/patronterms.pdf (accessed May 21, 2017) (OCLC privacy statement says, "OCLC does not provide personal information to any party except as required to do so by law. The Email Address and Name fields are specifically designed to collect personal information and are deleted before the transaction is saved or transferred. However, any information you provide in fields other than those, such as your question text, could be retained; therefore we encourage you to provide e-mail address and name, if used at all, ONLY in fields specifically designed for such information. You understand that while we do our best to protect your personal information, OCLC cannot ensure or warrant the absolute security of any information you transmit through this service. You agree that any information you provide on the web form and the text of your question are your sole responsibility and that you transmit information through this service at your own risk. Further, you understand how any personal information entered on the form may be used by the library or referral library and agree to that use.").

If you are looking to increase the security on your computer systems, Alison Macrina of The Library Freedom Project has several concrete suggestions for programs to use, and they are broken into larger groups as follows: Tor, browser safety, behavioral analytics, https, passwords, malware, full disk encryption, LUKS (GNU/Linux), mobile, e-mail, VPN's, terms of service, canaries and transparency reports, sandstorm, and operating systems.[130] Macrina and her team are also willing to assist you in setting up these tools, and do on-site workshops that can be tailored to specific groups like youth, LGBTQ, activists, and journalists.[131] Right now they are emphasizing their "First Library Digital Privacy Pledge" which focuses on "the use of HTTPS to deliver library services and the information resources offered by libraries. It's just a first step: HTTPS is a privacy requisite, not a privacy solution."[132]

Legislative Recommendations

Librarians have long been politically active and should lobby for legislative reform regarding the privacy of patron records. As we have seen, some states give only minimal protection, and two do not have statutory authority for protecting library records.[133] Arkansas has one of the most thorough statutes, and includes provisions like:

- ""Confidential library records" means documents or information in any format retained in a library that identifies a patron as having requested, used, or obtained

[130] Library Freedom Project, *Privacy Toolkit for Librarians,* https://libraryfreedomproject.org/resources/privacytoolkit/ (accessed May 21, 2017).
[131] Library Freedom Project, *Workshops,* https://libraryfreedomproject.org/ourwork/workshops/ (accessed May 21, 2017).
[132] Library Freedom Project, *The Library Digital Privacy Pledge,* https://libraryfreedomproject.org/ourwork/digitalprivacypledge/ (accessed May 21, 2017).
[133] Appendix A (Hawaii and Kentucky's Attorney Generals have read library patron record privacy into existing statutes about confidential statutes that do not specifically cover these records.).

specific materials, including, but not limited to, circulation of library books, materials, computer database searches, interlibrary loan transactions, reference queries, patent searches, requests for photocopies of library materials, title reserve requests, or the use of audiovisual materials, films, or records"[134]

- Criminal liability for illegal disclosures (misdemeanor)[135]
- Disclaimer of liability for lawful disclosure of records[136]
- "Public libraries shall use an automated or Gaylord-type circulation system that does not identify a patron with circulated materials after materials are returned"[137]
- Allows for the use of records to collect materials and fines[138]
- Allows for the use of records aggregate statistics for use by the library, if those records are scrubbed of personal identification[139]

The Arkansas statute is a good model for other states, although as technology changes, so too should the legislation regulating the use of it and the records it collects and how those records can be discovered and used.

VIII. Conclusion

The government has a long history of attempting to use librarians as informants, especially during times of political unrest and disagreement with the governing majority. The Trump administration has been subject to a great deal of criticism and there is growing dissent

[134] Ark. Code Ann. § 13-2-701 (2017).
[135] Ark. Code Ann. § 13-2-702 (2017).
[136] *Id.*
[137] Ark. Code Ann. § 13-2-703 (2017).
[138] Ark. Code Ann. § 13-2-705 (2017).
[139] *Id.*

among the populace for its policy changes. This country values free access to information and the pursuit of knowledge, and libraries not only facilitate intellectual pursuits, but also have become the guardians of the right to seek out information without fear of retribution.

Law libraries handle especially sensitive research records and are tasked with assisting people in times of great stress and anxiety. We have a duty to our patrons and to society to defend the right to research without intrusion.

APPENDIX A: 50 STATE SURVEY OF PRIVACY LAWS REGARDING LIBRARY RECORDS

State	Public **	Circulation records	Registration records	Reference q's protected	[Court] Order releases records**	Liability for illegal disclosures	Reports/stats discoverable **	Electronic/ digital info protected	"Any format" protected	Personal[ly] Identifiable Info protected**	Contained within FOIA**
Alabama	X	X	X				X		X		
Alaska	X				X					X	
Arizona	X				X	X		X7			
Arkansas	X	X		X	X	X	X	X		X	
California	X				X		X	X		X	
Colorado	X				X	X				X	
Connecticut	X1				X		X		X		
Delaware	X										X
DC	X	X			X	X					
Florida	X	X	X		X	X					
Georgia		X			X						
Hawaii	X	X									
Idaho						X				X	
Illinois	X	X	X				X				
Indiana	X									X	
Iowa	X				X3					X	
Kansas	X	X								X	
Kentucky	X	X	X								
Louisiana	X		X					X		X	
Maine	X				X		X			X	
Maryland		X								X	
Massachusetts	X									X	
Michigan					X	X					
Minnesota	X2				X					X	
Mississippi	X				X					X	

Missouri	X1				X4	civil	X	X		X	
Montana	X1				X5	X	X			X	
Nebraska	X									X	X
Nevada	X				X4	X				X	
New Hampshire					X		X	X		X	
New Jersey					X					X	
New Mexico	X	X	X		X	civil				X	
New York	X	X		X	X			X			
North Carolina					X					X	
North Dakota	X				X					X	
Ohio	X1			X	X		X	X		X	
Oklahoma	X				X				X	X	
Oregon		X									X
Pennsylvania	X	X			X6					X	
Rhode Island						civil			X	X	X
South Carolina	X	X	X		X4	X	X			X	X
South Dakota					X					X	
Tenessee	X1				X		X			X	
Texas	X				X4					X	
Utah	X				X					X	X
Vermont										X	
Virginia										X	X
Washington										X	
West Virginia	X	X			X						
Wisconsin	X				X					X	
Wyoming			X							X	X
Total	37	16	8	3	33	13	12	8	4	37	8

**if language was not exact, but the effect was the same, I included it
X1: open to the public
X2: explicitly only "government entities"
X3: finding of rational connestion between info and legitimate end
X4: finding that it is necessary to protect public safety or to prosecute a crime
X5: finding that public safety outweighs individual privacy
X6: only in a criminal proceeding
X7: e-books only

Appendix A:
State Privacy Laws Regarding Library Records (Citations)

Alabama
- Ala. Code § 41-8-9, 41-8-10 (West 2017).

Alaska
- Alaska Stat. § 40.25.140 (2017).

Arizona
- Ariz. Rev. Stat. Ann. § 41-151.22 (West 2017).

Arkansas
- Ark. Code Ann. § 13-2-701 to 13-2-706 (West 2017).

California
- Cal. Gov. Code Ann. § 6254, 6267 (West 2017).

Colorado
- Colo. Rev. Stat. Ann. § 24-72-204, 24-90-119 (West 2017).

Connecticut
- Conn. Gen. Stat. Ann. § 11-25 (West 2017).

Delaware
- Del. Code Ann. tit. 29 § 10002 (West 2017).

District of Columbia
- D.C. Code § 39-108 (West 2017).

Florida
- Fla. Stat. Ann. § 257.261 (West 2017).

Georgia
- Ga. Code Ann. § 24-9-40, 24-12-30 (West 2017).

Hawaii
- Haw. Atty. Gen. Op. 90-30 (Oct. 23, 1990) (available at http://oip.hawaii.gov/formal-opinions/90-30/)

Idaho
- Idaho Code § 74-108, 74-120 (2017).

Illinois
- 75 Ill. Comp. Stat. Ann. 5/1-7, 16/1-25, 70/1, 70/2, 140/7 (West 2017).

Indiana
- Ind. Code Ann. § 5-14-3-4 (West 2017).

Iowa
- Iowa Code Ann. § 22.7 (West 2017).

Kansas
- Kan. Stat. Ann. § 45-221 (2017).

Kentucky
- Ky. Atty .Gen. Op. 82-149, 1982 WL 176791 (Mar. 12, 1982).

Louisiana
- La. Rev. Stat. Ann. § 44:13 (2017).

Maine
- 27 Me. Rev. Stat. Ann. § 121 (2017).

Maryland
- Md. St. Govt. Code Ann. §10-616, 23-107 (2017).

Massachusetts
- Mass. Gen. Laws Ann. ch. 78 § 7 (West 2017).

Michigan
- Mich. Comp. Laws Ann. § 397.601 to 397.604 (West 2017).

Minnesota
- Minn. Stat. Ann. § 13.40 (West 2017).

Mississippi
- Miss. Code Ann. § 39-3-365 (West 2017).

Missouri
- Mo. Rev. Stat. Ann. § 182.815, 182.817 (West 2017).

Montana
- Mont. Code Ann. § 22-1-1101 to 22-1-1103, 22-2-1111 (2017).

Nebraska
- Neb. Rev. Stat. § 84-712.05 (2017).

Nevada
- Nev. Rev. Stat. Ann. § 239.013 (West 2017).

New Hampshire
- N.H. Rev. Stat. Ann. § 91-A:5, 201-D:11 (West 2017).

New Jersey
- N.J. Stat. Ann. 18A:73-43.2 (West 2017).

New Mexico
- N.M. Stat. Ann. § 18-9-1 to 18-9-6 (West 2017).

New York
- N.Y. Civ. Prac. Laws R. Law § 4509 (McKinney 2017).

North Carolina
- N.C. Gen. Stat. Ann. § 125-19 (West 2017).

North Dakota
- N.D. Cent. Code 40-38-12 (2017).

Ohio
- Ohio Rev. Code Ann. § 149.432 (West 2017).

Oklahoma
- Okla. Stat. Ann. tit. 65 § 1-105 (West 2017).

Oregon
- Or. Rev. Stat. Ann. § 192.502 (West 2017).

Pennsylvania
- 24 Pa. Consol. Stat. Ann. § 9375 (West 2017).

Rhode Island
- R.I. Gen. Laws § 11-18-32, 38-2-2 (2017).

South Carolina
- S.C. Code Ann. § 30-4-10, 30-4-15, 30-4-20, 60-4-10 to 60-4-30 (2017).

South Dakota
- S.D. Codified Laws § 14-2-51 (2017).

Tennessee
- Tenn. Code Ann. § 10-8-101 to 10-8-103 (West 2017).

Texas
- Tex. Govt. Code Ann. § 552.124 (Vernon 2017).

Utah
- Utah Code Ann. § 63G-2-202, 63G-2-302 (West 2017).

Vermont
- Vt. Stat. Ann. tit. 1 § 317 (2017).

Virginia
- Va. Code Ann. § 2.2-3705.7 (West 2017).

Washington
- Wash. Rev. Code Ann. § 42.56.310 (West 2017).

West Virginia
- W. Va. Code Ann. § 10-1-22 (West 2017).

Wisconsin
- Wis. Stat. Ann. § 43.30 (West 2017).

Wyoming
- Wyo. Stat. Ann. § 16-4-203 (West 2017).