WORLD LIBRARIES

Volume 26

No. 2

2022 worldlibraries.dom.edu/index.php/worldlib|

Public Libraries and Information Privacy Policies: A Case of the Naperville Public Library and Privacy Trends in the LIS Profession

Michael Kornfeind

Dominican University

ABSTRACT

The central role of technology in daily life undermines privacy. Many consumers accept data breaches, privacy violations and unauthorized access to confidential personal data as inevitable. However, the strict legal and ethical privacy guidelines governing public libraries demonstrates the importance of safeguarding privacy in the modern era. This case study of the Naperville Public Library analyzes internal privacy policies and includes a literature review of public library privacy issues in order to illustrate how libraries are fulfilling a commitment to privacy advocacy. The Naperville Public Library uses a series of privacy policies addressing adults, children and technology in order to outline how the library maintains patron privacy. This includes compliance with state and federal privacy laws with particular consideration to the Children's Online Privacy Protection Act (COPPA). Self-service hold areas, due data slips, cyberattacks, underdeveloped policies for IoT collections, third party vendors, chat platforms and eBook services represent key sources of privacy violations in public libraries. However, public libraries are also offering innovative privacy safeguards such as Virtual Private Network (VPN) services for library users and unique internal internet browsers embedded with robust cybersecurity features. Privacy audits, staff training, policy reviews and understanding how library vendors utilize patron data are key ways libraries can tackle privacy concerns.

INTRODUCTION AND BACKGROUND

Safeguarding privacy is particularly important in the modern digital era in which technology, smart devices, surveillance, data brokers, inadequate privacy laws and powerful tech firms are increasingly undermining privacy and the ability of sensitive personal information to remain confidential. The ubiquity of technology and data breaches has altered societal and individual expectations regarding privacy. Most people now accept privacy violations and unauthorized access to sensitive data as reasonable, legal and inevitable norms in the modern world (Wu, 2019). However, privacy is a reasonable expectation and considered a fundamental human

right by the United Nations. A lack of constitutional privacy protections in the United States is particularly troublesome when considering the existence of robust privacy-based regulations in Europe (Bennet, 2019). Privacy is also crucial because marginalized and underserved populations are frequently subject to disproportionately invasive privacy violations such as location tracking or surveillance (Madden, 2019).

Defining privacy and privacy-related concepts is key in order to highlight the complex challenges organizations encounter when crafting privacy policies or information security frameworks. The National Institute of Standards and Technology (NIST) (2021) defines privacy as the "assurance that the confidentiality of, and access to, certain information about an entity is protected." NIST (2021) further defines privacy as "the right of a party to maintain control over and confidentiality of information about itself." Furthermore, the privacy and cybersecurity scholar Roger Clarke (2016) defines information privacy as "the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves." Clarke further notes that information privacy includes safeguarding personal data and communications. The privacy posture of an organization and a privacy plan are also key elements of providing robust information security. Privacy posture is the status of an organization in terms of how its systems and internal resource are used to mitigate privacy risks and comply with privacy regulations (NIST, 2021). A privacy plan is a "formal document that provides an overview of the privacy requirements for an information system or program and describes the privacy controls in place or planned for meeting those requirements. The privacy plan may be integrated into the organizational security plan or developed as a separate plan" (NIST, 2021).

Public libraries in the United States are staunch privacy advocates and utilize a variety of methods to protect the privacy of library users. As community resource centers and information hubs, public libraries must navigate complex privacy and confidentiality

considerations in order to provide library users with robust information services and equitable access to resources. Privacy policies utilized by public libraries must balance legal, ethical and professional privacy frameworks. Information privacy in the public library sphere is particularly complex because it involves the interplay and potential conflicts between organizational, user and legal expectations regarding privacy. This paper will examine the information privacy policies of the Naperville Public Library. The library retains three privacy-related policies: a confidentiality and privacy policy, internet and computer use policy, and children's privacy policy. Analyzing these three policies will reveal if the library is providing robust information privacy safeguards for library users. A brief overview of methodology and an analysis of the library's privacy policies will identify how the library protects user privacy. Evaluating current literature regarding privacy protections in public libraries, identifying gaps in library security policies, examining the impact of privacy laws and outlining potential solutions will provide insight into how the Naperville Public Library can better tackle privacy issues. Ultimately, this case study will provide library users and library and information science (LIS) professionals with insights into how libraries can address privacy through policies, cybersecurity measures and compliance with legal frameworks.

METHODOLOGY

This paper will utilize a case study approach to analyze how the Naperville Public Library addresses privacy. Case studies are a qualitative research method focusing on the descriptive evaluation of a small group or population in order to identify key points in the unique context of a specific organization. Cumulative case studies collect data from distinctly different time periods and samples in order to more efficiently obtain more applicable generalizations. Exploratory case studies precede larger inquiries and primarily focus on identifying relevant questions and measurement metrics. The strengths of case studies include flexibility regarding research methods and robust insight into the unique organizational context of a studied participant group. A weakness of case studies stems from a lack of subjectivity by researchers

because personal inferences about data may generate results that are not valid or generalizable. Other weaknesses include personal bias, unethical funding sources, high research costs and time-intensive timelines (Becker et al., 2021).

This paper will use an illustrative case study approach, which will provide a descriptive assessment of privacy policies at the Naperville Public Library and its impact on users. Data collection will focus on library documents and archival materials. An assessment of library documents, news articles, related LIS literature and privacy laws will provide a lens for evaluating the efficacy of privacy protections used by the Naperville Public Library. Lastly, data analyses will examine key themes or practices used by the library in comparison to overarching trends in the profession and in terms of compliance with privacy guidelines from across the world (Becker et al., 2021).

RESULTS

Research does not indicate any publicly accessible records of privacy violations at the Naperville Public Library. However, there are several common types of information privacy violations unique to public libraries. Many libraries utilize chat platforms to facilitate reference services. Chat platforms spur privacy issues because most of them require patrons to input personally identifiable information (PPI) such as name, email address, phone number and the content of reference questions. An uptick in chat sessions due to the pandemic led the Hilton C. Buley Library at Southern Connecticut State University to recognize the privacy issues associated with chat platforms. The library addressed this privacy violation by updating settings of their chat service to make inputting PPI optional for users. They also updated privacy policies to include the unique privacy issues associated with chat platforms (Fruehan & Hellyar, 2021).

Due date slips also represent a source of privacy violations in public libraries. Due date slips frequently contain sensitive information such as name, phone number, email address, library

card number and item information. This exposes confidential patron library records to the public. A survey of fifty-five Canadian public libraries found most libraries protect privacy and only include information like date due, titles of borrowed items and library name on due date slips. However, survey results indicate that 13% of surveyed libraries with staffed service points generate due date slips with patron names included and 1.9% of libraries also placed email addresses and phone numbers on due date slips (Hung, 2014).

An analysis of public libraries in Ontario, Canada revealed that many libraries are providing inadequate privacy protections. The study highlights that most libraries fail to meet government privacy regulations, notify patrons about the use of personal information or satisfy American Library Association (ALA) privacy guidelines. Public libraries in Ontario fail to openly disclose how patron personal information is utilized and stored. This includes a lack of access to privacy policies and failure to provide patrons with notifications regarding how their personal information is used. Furthermore, the study shows that many public libraries in Ontario do not engage in sufficient compliance practices aligned with government privacy regulations (Burkell & Carey, 2011).

Self-service holds represent another controversial source of privacy violations in public libraries. Public libraries using self-service hold systems violate many state-level privacy laws by placing confidential patron library records in the public sphere. This provides public access to individual borrowing habits and item titles which can reveal sensitive medical issues or legal troubles. Hold slips may also include sensitive PPI such as name, email address or library card number. Self-service holds demonstrate a dilemma of convenience versus privacy. The system also may allow law enforcement officials to engage in surveillance and circumvent subpoenas. Self-service holds are convenient and popular, but undermine privacy protections libraries are supposed to staunchly maintain (Bowers, 2008).

Public libraries are also frequently targeted by cyber attackers. In November 2021 the Toledo Lucas County Library was the victim of a cyberattack which rendered all technology and devices connected to library networks inoperable (Daniely, 2021). In August 2021 the Boston Public Library experienced a cyberattack which downed public computer, printing and digital resource services. The library worked with city officials and law enforcement agencies to investigate the attack. However, the attack forced the library to rebuild multiple systems and led to the loss of patron transaction data (Boston Public Library, 2021).

The information privacy context of the Naperville Public Library primarily stems from a series of privacy policies and rules. The organization views information privacy according to state and ALA privacy frameworks. Information technology (IT) staff members address cybersecurity and network security components of privacy enforcement. Library managers and administrators in conjunction with library legal counsel handle law enforcement requests, court orders and privacy violations. The human resources department is also a key component in confidentially managing and storing sensitive data about employees. However, all library employees including paraprofessionals and librarians are required to comply with privacy policies and legal guidelines. This is important when considering that library staff handle patron data during numerous daily interactions such as reference interviews, program registrations, interlibrary requests or circulation transactions.

Naperville Public Library primarily addresses privacy through three privacy policies. The Confidentiality and Privacy Policy reiterates the Illinois Library Records Confidentiality Act. The library defines sensitive identifying information as addresses, phone numbers, birth dates and personal identifiers. The policy notes the library will comply with the USA Patriot Act or search warrants issued by an FBI agent. Web site privacy is also addressed. The library notes that it will

not sell or share patron web data to third parties. Anonymous statistical records are kept such as usage reports regarding network volume and traffic. Patron account information is not available to database vendors when using digital resources. The library does log some patron web data such as IP address and browser type (Naperville Public Library, 2017a).

The Children's Privacy Policy highlights that the library collects personal information about children to register them for events or services. This includes data like name, birth date, address, email address, library card number, school, grade level, emergency contacts and scheduling availability. The policy emphasizes that the library does not disclose personal information about children to vendors or third parties. An exception is businesses or organizations used to facilitate programming events, which represents a privacy risk. The policy also includes compliance metrics with the Children's Online Privacy Protection Act (COPPA) and parental consent rights (Naperville Public Library, 2017b).

The Internet and Computer Use Policy addresses key privacy risk areas. Computers in the children's area offer filtered internet access and children under the age of eight require a parent or guardian to access computers. The policy highlights the risks of using the library's unsecured Wi-Fi network. Patrons are not allowed to view or produce sexually explicit material, which some patrons may challenge as a privacy violation and an impingement of constitutional rights. The policy notes patrons cannot use public computers to engage in libel, slander, misrepresentation, bullying or harassment. Some patrons may consider these privacy violations by challenging individual freedom of speech and intellectual freedom. Dictating how patrons use public computers could potentially be seen as an attempt to regulate speech. Another privacy issue is that sensitive information sent to public printers may compromise privacy. Similarly, conducting banking or other sensitive transactions using library Wi-Fi or public computers poses risks associated with identity theft, cybercrime or compromised data confidentiality (Naperville Public Library, 2020).

DISCUSSION

The privacy perspectives of Naperville Public Library are strongly influenced by overarching ALA privacy guidelines. This is evident in the language, structure and scope of the privacy policies created by the library. The library closely follows the frameworks and privacy protections recommended by the ALA with consideration to multiple demographic populations and a separate policy for technology use. The ALA characterizes privacy and ensuring the confidential use of library resources as fundamental protections of constitutional rights such as free speech, free thought and intellectual freedom. Maintaining robust privacy and confidentiality safeguards are a central component of library services. Library users should expect complete confidentiality regarding "information sought or received and resources consulted, borrowed, acquired or transmitted" (ALA, 2006). Libraries do not record, store or assign personal identifiers related to circulation records, reference transactions, interlibrary loan requests, database access, program attendance or internet activity. The ALA provides numerous guidelines for libraries regarding how to create privacy policies, engage in digital security, coordinate with law enforcement inquiries and comply with applicable state confidentiality laws. Many public libraries include separate private guidelines for adults and children. State privacy laws vary, so the ALA recommends incorporating state privacy regulations into library policies in order to ensure compliance. The ALA (2007) notes that "materials subject to privacy and confidentiality restrictions may include online search histories, database search records, ILS records or other circulation records, interlibrary loan records, and all other personally identifiable uses of library materials, facilities, programs or services, such as reference interviews." The ALA outlines how and when libraries should provide private user information to law enforcement agencies. Federal agencies or police agencies are unable to legally demand and access library user records. Libraries will not provide sensitive user data without permission from individual library users or in compliance with judicial orders (ALA, 2021).

Several privacy laws serve as the foundation of the privacy policies of the Naperville Public Library. The primary legal influence is the Illinois Library Records Confidentiality Act, which stipulates that registration and circulation records are confidential and not subject to disclosure to third parties. Libraries may disclose library records due to a court order or law enforcement emergency, but disclosures are limited to identification purposes. The law notes that libraries are able to publish statistical reports based on patron data. Cooperating with lawful requests from law enforcement is also not considered a breach of confidentiality (FindLaw, 2019). The other primary law shaping the privacy policies of Naperville Public Library is the Children's Online Privacy Protection Act (COPPA). This legislation is enforced by the Federal Trade Commission (FTC) and outlines rules governing websites that provide services (and collect data about) for children under the age of twelve. COPPA compliance metrics include posted privacy policies, direct notifications sent to parents, parental consent, a parental review process, rights to revoke consent and data security protocols (Federal Trade Commission, 2002). The Naperville Public Library meets and enforces all COPPA requirements through the rules of the Children's Privacy Policy. It is also important to note that school and public libraries are incentivized to uphold privacy safeguards such as the Children's Internet Protection Act (CIPA) because compliance with enforcement is tied to the E-rate program which provides federal funding and discounted technology resources (National Conference of State Legislatures, 2020). It is evident that the rules and policies shaping privacy protections at the Naperville Public Library are robust and bolstered by strong legal precedents.

Europe has spearheaded some of the most innovative information privacy protection legislation in history, which provide examples of how to improve privacy in public libraries. The General Data Protection Regulation (GDPR) is a series of legal rules in Europe addressing data protection and digital privacy. The rules provide consumers with robust autonomy regarding how personal data is used and accessed by organizations. It also provides compliance regulations and fines to ensure companies are accessing, storing and disseminating personal data according to GDPR guidelines. Consumer protections include mandatory data breach notifications, opt-in rights,

transparency regarding how personal data is processed and the right to erase personal data records to safeguard anonymity (Palmer, 2019).

Information privacy protections in public libraries are undermined by a lack of robust overarching privacy laws in the United States. A lack of meaningful federal-level privacy protections for consumers is a national policy failure. Unfortunately, ineffective federal privacy laws are able to pre-empt and undermine stronger state-level protections. However, some U.S. states offer privacy protections that are also evident in the GDPR. For instance, the California Consumer Privacy Act offers the strictest privacy rules in the U.S. and allows consumers to block third party sales of personal information (New York Times Editorial Board, 2019c). The act provides consumers with rights regarding how personal information is collected, why personal data is collected and how consumer data is disseminated to third parties. This empowers consumers by allowing them to sue companies for data breaches or privacy violations, which relieves the state attorney general of overwhelming enforcement responsibilities (favoring corporations due to limited prosecutorial resources). Californian legislators characterize the legislation as providing consumers with enforceable privacy rights which counteract the numerous exemptions companies typically utilize to avoid regulatory oversight. The act also aims to protect constitutional privacy rights for consumers (Cowan, 2019).

Several themes are evident when analyzing the commonalties between various information privacy frameworks. Compliance, enforcement and accountability are common principles, which are typically enforced with fines or penalties for violating data protection protocols. Transparency, consumer consent, opt-in rights and the ability to request how organizations are using personal data are also common elements. Many information privacy and data protection laws allow consumers to correct or update personal information. Strict limitations are also a commonality, particularly regarding how data is collected and what type of sensitive data is acceptable to access.

Library users face several privacy challenges when using library services at the Naperville Public Library. The Internet and Computer Use Policy may undermine freedom of speech and intellectual freedom by regulating what content patrons can access online. Public computers with cookies, shared browser histories and saved personal data represent privacy risks as does using unsecured public Wi-Fi networks (Naperville Public Library, 2020). Sensitive patron data may also be compromised by vendors used by the library such as database providers, journal publishers or streaming applications.

Digital book services, eBooks and digital content also generate unique and significant privacy issues for public libraries. Libraries safeguard privacy by collecting minimal personal information about library users. However, digital book services collect vast amounts of data about readers, which is then accessible to government agencies or third parties. Federal and state legal precedents include several instances of protecting reader privacy in order to safeguard privacy, individual rights and freedom of expression. Library policies and regulations advocate for strict confidentiality and privacy rules regarding patron reading habits, circulation records and library activity. Digital book services circumvent these privacy safeguards and collect vast amounts of personal information about readers such as search queries, borrowing history, location, IP address, reading speeds, margin notes, and other personal data. People using Google or Amazon digital reading services are subject to further invasions of privacy because the companies can track interconnected activity like email or social media usage and repackage personal data to digital advertisers (Ozer, 2010).

RECOMMENDATIONS

Several improvements could bolster the information privacy practices utilized by the Naperville Public Library. Library administrators should incorporate privacy as a key pillar of the next

strategic plan. This should include goals, metrics and timelines related to expanding privacy-based initiatives. For example, staff training focused on properly handling sensitive personal patron information and awareness of applicable privacy laws. There are several online training modules available for libraries which focus on privacy literacy training. Programming events should also be used to expand privacy awareness and knowledge in the community. The library could host workshops with cybersecurity or legal experts providing information about privacy, digital privacy, legal rights, privacy-related issues and how to engage in digital minimalism. Privacy audits would also be an effective way for the library to identify gaps in current information privacy protections. The library should map how privacy is managed at each service point and level of the organization. Auditing also requires identifying data flow and storage processes, testing staff knowledge about privacy compliance, expanding cybersecurity safeguards, implementing access controls, utilizing the principle of least privilege when handling patron data and evaluating how library vendors store patron data (ALA, 2014).

Using interactive training sessions and role-playing would better inform staff at Naperville Public Library about how to address privacy concerns. The library currently relies on policies and some training initiatives, but could significantly increase staff privacy training. Snowman (2013) illustrates how scenario training can bolster the curriculum of staff training initiatives. This requires first providing staff with an overview of ethical, professional, legal and internal privacy guidelines. Scenario training includes presenting library staff with interactive scenarios related to privacy issues with discussion points and debriefing sessions. This can helpfully show staff how to handle privacy-related issues such as casual law enforcement inquiries, subpoena requests, safeguarding children's accounts, account history disclosures, parental consent and how to ensure confidentiality of data. Using interactive training sessions and role-playing would better inform staff at Naperville Public Library about how to address privacy concerns (Snowman, 2013).

Examining innovative information privacy practices utilized by other public libraries highlights additional methods the Naperville Public Library could implement to bolster privacy safeguards. For instance, The Palm Beach County Library System created its own internet browser for public computers in order to better safeguard confidentiality and privacy. Many internet browsers on public access computers generate significant privacy concerns such as cookies, saved browsing histories, autocomplete forms and saved passwords. Typical privacy protocols such as kiosk modes offer limited browser functionality. Incognito modes or deleting browser histories are also often ineffectual privacy practices which can be easily circumvented. The library used Microsoft Visual Studio Express for Windows Desktop to create a unique internet browser. The new browser offers more robust cybersecurity options such as auto-deleting files, managing temporary files, data overwriting functions and disk sanitization (Brandt, 2016). Naperville Public Library should also consider offering free open access virtual private network (VPN) services to patrons to bolster privacy and cybersecurity. LibraryVPN is an example of the innovative privacy and cybersecurity practices implemented by public libraries. LibraryVPN is an open-source application being piloted by public libraries in the eastern United States which provides library users with free access to a secure VPN. Patrons download an application to a device and use their library card to access secure VPN services. This illustrates how public libraries are providing patrons with privacy protections and equitable access to cybersecurity tools (McAndrew, 2020).

Lastly, Naperville Public Library should consider creating a separate privacy policy addressing the internet of things (IoT). The library possesses numerous technology-based collections such as the Tech Buffet, a sound recording studio, video production room, borrowable devices, creative software and other connected devices (Naperville Public Library, 2021). An IoT privacy policy should include rules such as avoiding storing user data on third-party systems and deleting user data after a certain period of time, which helps mitigate risks associated with future data breaches. Libraries should also disclose privacy policies and guidelines to users accessing IoT resources. Challenges of securing IoT include weak authentication protocols

available for connected devices. Libraries also need to request vendors such as database or journal providers disclose how they access, use and store data collected about library users. This entails auditing the cybersecurity practices of third-party services used by libraries. Strong encryption protocols to safeguard network traffic for IoT are also key. Many devices utilize location services and tracking, which can violate the privacy of library users. Libraries should disable location tracking, offer an opt-in option and work with developers to ensure that personal identifiers are stored only when necessary. These security protocols help safeguard the privacy of library users, reinforce the confidentiality of data and avoid unauthorized surveillance (Hahn, 2017).

LIMITATIONS

Several limitations are evident in this case study. More sources could be used to bolster data collection efforts. For example, including interviews, direct observation and participant observation (staff or patrons) would provide more qualitative data. This study primarily used primary sources and internal library documents, which represents a significant limitation. Another limitation is that Naperville Public Library doesn't offer open access to data regarding privacy-related data breaches or violations, which led to this study using privacy issues from other public libraries to formulate inferences. Visiting branches of the Naperville Public library and observing staff or patrons would help provide more context regarding the role of privacy during typical library interactions. Interviews with staff and patrons could also help identify privacy concerns or gaps in privacy policies. This data could be coded and subject to quantitative analyses which would better highlight overarching themes related to privacy, cybersecurity and confidentiality. Surveys could be used to bolster the qualitative research methods of this study. For example, surveying both staff and library users would provide invaluable insights into privacy concerns, practices and topics. This could also be used to ascertain if staff onboarding or professional development training provides an adequate amount of knowledge about privacy laws and how to handle sensitive patron information. A

survey would consist of multiple choice, checklist, open-ended and scaled-response question formats. Using a combination of mail and email surveys would be used to obtain a robust response rate. A stratified random sample approach would be utilized to obtain a respondent pool representative of Naperville's population demographics. For example, various school age groups, senior citizens, middle aged adults, families and other key categories will be proportionately represented in the survey results (Matthews, 2018, pp. 55-58).

CONCLUSION

The central role of technology in daily life increasingly undermines privacy protections. Data brokers, data breaches, tech firms and smart devices represent some of the issues associated with privacy in the modern world. Public libraries are staunch privacy advocates and operate according to strict government and ALA privacy guidelines. An illustrative case study of the Naperville Public Library illustrates that the library uses a series of policies to implement privacy safeguards. Compliance with state and federal laws as well as additional privacy measures regarding children are evident. However, the case study suffered from some limitations such as a lack of interviews, surveys or direct participant observation at library branches. Additionally, there is little research regarding privacy violations at the Naperville Public Library, which led to a more general review of the literature concerning privacy violations in public libraries. Self-service hold areas, due data slips, cyberattacks, underdeveloped policies for IoT collections, third party vendors, chat platforms and eBook services represent key sources of privacy violations in public libraries. The robust information privacy policies of the Naperville Public Library embody best practices in the profession by balancing public, institutional and government privacy laws. Strong policies also provide transparency for patrons (Nichols Hess et al., 2015). However, the library could improve privacy protections by pursuing privacy audits, offering interactive staff privacy training, providing patrons with VPN services and crafting a privacy policy for IoT collections. The ubiquity of technology and increasing power of tech firms suggests that expectations of privacy will continue to erode as people accept data breaches and

the unregulated monitoring of sensitive personal information as acceptable social norms. Amidst this new privacy dynamic in society public libraries represent a hopeful source of privacy advocacy and innovative privacy safeguards which benefit communities and create safes spaces in which library users can securely access knowledge and resources.

REFERENCES

American Library Association. (2006, July 07). Privacy: *An Interpretation of the Library Bill of Rights*. https://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy

American Library Association. (2007, May 29). State Privacy Laws Regarding Library Records. https://www.ala.org/advocacy/privacy/statelaws

American Library Association. (2014, April 25). Privacy Audits. https://www.ala.org/advocacy/privacy/audits

American Library Association. (2014, April 25). Training & Programming. https://www.ala.org/advocacy/privacy/training

American Library Association. (2021, October 28). Law Enforcement Inquiries – Key Concepts. https://www.ala.org/advocacy/privacy/lawenforcement/inquiries

Becker, B, Dawson, P., Devine, K., Hannum, C., Hill, S., Leydens, J., Matuskevich, D., Traver, C., & Palmquist, M. (2021). Designing and Conducting Case Studies. *Colorado State University.* https://writing.colostate.edu/guides/guide.cfm

Bennet, J. (2019, April 10). Do You Know What You've Given Up? *The New York Times*. https://dominicanu.instructure.com/courses/1695076/files/206579121/download?wrap=1

Boston Public Library. (2021, August 27). Statement from the Boston Public Library: Technical Outage. https://www.bpl.org/news/statement-technical-outage/

Bowers, S. L. (2008). Self-Service Holds: A Violation of Library Patrons' Privacy. *Public Libraries*, *47*(4), 54–57.

Brandt, P. (2016). A BETTER BROWSER EXPERIENCE: UX Meets Patron Security and

Confidentiality. *Computers in Libraries*, *36*(8), 4–7.

Burkell, J., & Carey, R. (2011). Personal Information and the Public Library: Compliance with Fair Information Practice Principles. *Canadian Journal of Information & Library Sciences*, *35*(1), 1–16.

Clarke, R. (2016, July 24). Introduction to Dataveillance and Information Privacy, and Definitions of Terms. http://www.rogerclarke.com/DV/Intro.html#InfoPriv

Cowan, J. (2019, May 22). The Fight Over a Landmark Digital Privacy Law. *The New York Times*. https://dominicanu.instructure.com/courses/1695076/files/206579033/download?wrap=1

Daniely, Willie. (2021, November 03). Toledo Lucas County Public Library recovering from cyber attack. *WTVG*. https://www.13abc.com/2021/11/04/toledo-lucas-county-public-library-recovering-cyber-attack/

The Editorial Board. (2019c, June 08). Why Is America So Far Behind Europe on Digital Privacy? *The New York Times*. https://dominicanu.instructure.com/courses/1695076/files/206579035/download?wrap=1

Federal Trade Comission. (2002). Protecting Children's Privacy Under COPPA: A Survey on Compliance. https://www.ftc.gov/sites/default/files/documents/rules/children%E2%80%99s-online-privacy-protection-rule-coppa/coppasurvey.pdf

FindLaw. (2019, January 01). Illinois Statutes Chapter 75. Libraries § 70/1.Registration and circulation records; statistical reports. https://codes.findlaw.com/il/chapter-75-libraries/il-st-sect-75-70-1.html

Fruehan, P., & Hellyar, D. (2021). Expanding and Improving Our Library's Virtual Chat Service: Discovering Best Practices when Demand Increases. *Information Technology & Libraries*, *40*(3), 1–9. https://doi.org/10.6017/ital.v40i3.13117

Hahn, J. (2017). The Internet of Things: Mobile Technology and Location Services in Libraries. Library Technology Reports, 53(1), 1–28. https://doi.org/10.5860/ltr.53n1

Hung, J. T. (2014). Giving the Slip: A Study of the Format and Content of Date Due Slips in Canadian Public Libraries. *Partnership: The Canadian Journal of Library & Information Practice & Research*, *9*(2), 1–16. https://doi.org/10.21083/partnership.v9i2.3114

Madden, M. (2019, April 25). The Devastating Consequences of Being Poor in the Digital Age. *The New York Times*. https://dominicanu.instructure.com/courses/1695076/files/206579013/download?wrap=1

Matthews, J. (2018). *The Evaluation and Measurement of Library Services* (2nd ed.). Libraries Unlimited.

McAndrew, C. (2020). LibraryVPN: A New Tool to Protect Patron Privacy. *Information Technology & Libraries*, *39*(2), 1–3. https://doi.org/10.6017/ital.v39i2.12391

Naperville Public Library. (2017a, January 18). Confidentiality and Privacy Policy. https://www.naperville-lib.org/sites/default/files/pdf/Policies/policy230.pdf

Naperville Public Library. (2017b, September 20). Children's Privacy Policy. https://naperville-lib.org/sites/default/files/pdf/Policies/Children's%20Privacy%20Policy.pdf

Naperville Public Library. (2020, December 16). Internet and Computer Use Policy. https://www.napervillelib.org/sites/default/files/pdf/Policies/Internet%20and%20Computer%20Use%20Policy.pdf

Naperville Public Library. (2021). Resources – Computers & Technology. https://www.naperville-lib.org/research/computers-technology

National Conference of State Legislatures. (2020, July 10). *Children and the Internet: Laws Relating to Filtering, Blocking and Usage Policies in Schools and Libraries*. https://www.ncsl.org/research/telecommunications-and-information-technology/state-internet-filtering-laws.aspx

National Institute of Standards and Technology. (2021). Privacy. *Computer Security Resource Center*. https://csrc.nist.gov/glossary/term/privacy

National Institute of Standards and Technology. (2021). Privacy posture. *Computer Security Resource Center*. https://csrc.nist.gov/glossary/term/privacy_posture

National Institute of Standards and Technology. (20210. Privacy plan. *Computer Security Resource Center*. https://csrc.nist.gov/glossary/term/privacy_plan

Nichols Hess, A., LaPorte-Fiori, R., & Engwall, K. (2015). Preserving Patron Privacy in the 21st

Century Academic Library. The Journal of Academic Librarianship, 41(1), 105–114. https://doi.org/10.1016/j.acalib.2014.10.010

Ozer, N. (2010). Digital Books: A New Chapter for Reader Privacy. *American Civil Liberties Union of Northern California*. https://www.aclunc.org/sites/default/files/asset_upload_file434_9996.pdf

Palmer, D. (2019, May 17). What is GDPR? Everything you need to know about the new general data protection regulations. *ZDNet*. https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/

Snowman, A. (2013). Privacy and Confidentiality: Using Scenarios to Teach Your Staff About Patron's Rights. Journal of Access Services, 10(2), 120–132. https://doi.org/10.1080/15367967.2012.762267

Wu, T. (2019, April 10). How Capitalism Betrayed Privacy. *The New York Times*. https://dominicanu.instructure.com/courses/1695076/files/206579061/download?wrap=1