What Privacy? Online Privacy Culture and the Role of Libraries in Digital Information Literacy

HANNAH LEE

The COVID-19 pandemic revealed how modern society requires online connectivity to function, and it also revealed many cracks in internet data sharing and privacy issues. When internet society first developed in the early 2000s, few could have predicted how much data and privacy individuals would relinquish for the sake of easy access to information and products. In modern times, technology companies make sharing and connecting through the different online apps and platforms simple, and it is hard to imagine using an app without an option to log in through Apple ID, Google, or Facebook. Prominent tech companies like Facebook, Twitter, Apple, and Amazon so often misuse and abuse their users' data that privacy breaches are almost the norm rather than the exception. Many of the services these companies provide do not cost money to use; however, the tradeoff for utilizing social media platforms and tech companies' free services is the willingness to have one's user data sold. But what data are individuals providing to tech companies? Is the user's data legally protected? In the United States, legislation meant to protect privacy stems from the decades-old Digital Millennium Copyright Act (1998) or, more recently, the California Consumer Privacy Act (CCPA) of 2018. However, legislation can do little if people do not know their digital information and privacy rights, which are often buried under complex legalese in end-user license agreements.

Librarians in higher educational institutions are in a unique position of understanding digital privacy issues by working with individuals' data, configuring library services, and discussing library and information science scholarship. Historically, libraries have valued patron privacy as a foundation of intellectual freedom (American Library Association, 2002) and strive to protect this privacy. While many libraries have been forced to comply with searches requiring libraries to disclose patron information (e.g., warrants, Patriot Act), some libraries have also warned patrons about such possibilities (Matz, 2008; Starr, 2004). Academic libraries have additional laws to comply with, compared to public libraries, where privacy laws in higher education impact students via FERPA. FERPA (Family Educational Rights and Privacy Act, 1974) guarantees that a student's educational privacy transfers from parent to student at 18 years old. Even though institutions may follow FERPA to the letter of the law and might try to comply and protect students' privacy data, the actual practice of FERPA is not always possible in a digital economy (Abbott, 2022; Brown & Klein, 2020; Inouye & Agnello, 2015; Lowenstein, 2016; Schrameyer et al., 2016).

Patron privacy in libraries has changed over the decades, modeling technological advances in libraries. As libraries shifted from being paper-based to technology-based, libraries have become more reliant on digital tools and services to meet community demands, with one prominent example being the development of open public access catalogs (OPACs). Today's complex discovery tools require multiple vendors and integrations, combining library services with a digital environment that includes restrictions like copyright, technical limitations, and data privacies.

The value of patron information is not limited to the sphere of higher education. While there is an emphasis in higher education on the value of information that comes from publication or research, individuals produce valuable information (Association of College & Research Libraries, 2015) as members of society. Being an informed citizen of online society means being aware of the value of our private information, what rights we give away, why we give our privacy away, and the consequences of our actions. The focus of this chapter is to reflect on the invasive state of current data privacy practices and how librarians in higher education can be an information source for privacy rights.

https://doi.org/10.56638/mtopb00123

Background

The dictionary definition of privacy is simple in that there is an expectation of "being alone, undisturbed, or free" from attention (Oxford University Press, n.d.). Scholars debate the nature of privacy and the agency that individuals have in controlling information about themselves or freedom from external intrusion (ALA Office for Intellectual Freedom, 2010; Bélanger & Crossler, 2011; Campbell & Cowan, 2016; Kenyon & Richardson, 2006; Rotenberg et al., 2015; Sloot & Groot, 2018). The implications of individual privacy have evolved alongside technology and documentation methods.

Maintaining one's privacy was much easier before the computer age. Unless explicitly spoken, written, or observed in public, individuals did not have to worry too much about exposing their private information to the world. Without efforts to maintain memories through writing, visual media, or oral traditions, memories were short-lived. Even with early cameras and recording devices, there was a barrier of entry to have access to these tools. Either processing film took a long time, or the equipment was too expensive for the average person.

Libraries and Privacy

During this pre-computer era, libraries were limited by the ability to keep physical records. Using check-out cards and due date slips, books and other media checked out from the library could be traced back to its user through a patron's handwritten name or ID (Surace, 1970). However, patron privacy could easily be preserved by writing over names on the checkout cards or eliminating paperwork linking patron IDs to the material. This era of library circulation would also require a deeper search to connect patrons to their checked-out material; someone would need to find the original book to link it to an individual. If there were multiple copies of the same item, then there would be the additional complication to link to the same copy that a patron checked out. However, privacy in libraries began to change with the introduction of public computers.

One of the places people were able to gain access to computers in the early days of the internet was the library. Starting with early computers intended to help with basic functions like payroll and accounting, there was growing recognition for more complicated tasks using computers (Allen, 2014; Arms, 2012). In the 1960s, the Library of Congress investigated the possibility of a machine-based form of information storage and retrieval, eventually giving the library sciences what is known today as Machine Readable Cataloging, or MARC (Avram, 1975). While libraries had library classification systems like the Dewey Decimal System (in many public libraries) or the Library of Congress Call Number System (in many academic libraries), it was difficult to search for items unless you knew the subject-based term needed to begin the search. Even card catalogs did not have a standard means of organizing; while sorting by the author's last name was common, it was not the only method of card catalog organization (Pachefsky, 1969). These physical organization discrepancies would lead to the development of computer-based catalogs to aid in searching.

Soon after the Library of Congress considered (and approved) the idea of using MARC came the Online Public Access Catalog (OPAC). Although the term "OPAC" came into use in the 1980s, the basic idea was to have a public-facing (i.e., patron-accessible) catalog of a library's holdings (Wells, 2020). Most of the early OPACs concentrated on providing local records for local patrons; in other words, you could only search for things using the library's OPAC in the library where you were physically located (or call to ask).

The OPAC made searching via keywords easier, but the growth of the internet and the availability of different types of information required complex systems to address an increasingly complex digital information society. This complexity brought on the need for what libraries call "discovery systems." Discovery systems allowed patrons to go beyond a local library's catalog record to enable basic functions present in internet searching (e.g., spelling corrections, autofill suggestions) while connected to previously separate systems like databases. Instead of searching specific databases for

scholarly articles (requiring some level of working knowledge of each discipline or databases in general) and a separate system for the library catalog, discovery systems allowed for multiple functions from a single platform (Dahl, 2009; Giza, 2022). The interconnectedness of discovery systems often happens through single sign-on (SSO) credentials and proxies tied to an individual's email or school username. However, if systems do not have built-in mechanisms anonymizing users' data, then privacy breaches can occur. Libraries can link individual users with their network access, especially as databases are trying to curtail piracy and track users through proxy networks. While discovery systems make accessing information convenient through a single portal, the library and its librarians must ensure that patron privacy remains intact.

The library profession advocates for patron privacy as a part of its Bill of Rights (American Library Association, 2002), but digital technologies add challenging layers (Gardner, 2002; Hess et al., 2015). With the increase in technical functionality of libraries came an accompanying increase in digital privacy innovations and accompanying concerns. Rather than using physical checkout cards, books and other materials now have barcodes linked to electronic records. With digital recordkeeping, libraries take care to only keep records of what patrons check out *while* the items are checked out; typically, the default for OPAC and discovery systems is to delete (or destroy) a patron's checkout history. While there are metrics in place to show how many times a single item may have circulated, library systems do not connect them to the patron (Klinefelter, 2007; Pekala, 2017).

Even with access to electronic resources like eBooks, journal articles, databases, and other electronic materials paid for by the library, these systems often tie a username or library card number with a limit to how long that record exists. Typically, through the use of proxy networks capable of authenticating access to electronic resources, a patron can get access without giving too much personal information. Of course, if the patron's ID username is easily identifiable (e.g., firstname.lastname), identifying individuals would be easy if not for the technical limits of how long libraries keep patron information (Murray, 2001; Shabtai et al., 2013; Wang et al., 2016).

As interoperability and ease of access to various platforms grow, the library is one of the few places that does not tie usage to a social media platform. Libraries have their own social media accounts for marketing purposes, but a patron would not be able to "Login using Facebook" or "Use your Google Account" as options for logging in to library services. While the minimum for obtaining a library card is typically an email address (more for notifications and as a means of contacting), libraries do not connect with a patron's social media to build a profile in the same way a technology company develops large datasets.

This separation of social media and library accounts means individuals can keep their library habits private without worrying that libraries will sell their information or similarly disclose their information. In an internet era requiring so much disclosure of personal information, dedication to privacy means that libraries are a place where individuals can seek knowledge with assured privacy protections (Cooke, 2018; Rubel, 2014). Privacy in libraries becomes a critical component of personal freedoms, particularly for marginalized people or people in communities actively censoring information (Spilka, 2022).

That is not to say that privacy invasions do not occur. A study of public libraries and library vendors found that many vendors did not meet the professional standards for using and handling users' information (Lambert, et al., 2015). Additionally, a 2010 study also revealed the same concerns about vendors, adding that although library vendors were transparent about their practices, little could be done by library patrons or libraries (Magi, 2010). However, more recent studies show that library vendors are catching up to the privacy needs of libraries and their users (McKinnon & Turp, 2022; Yoose, 2017). Although additional studies should be done in the future to ensure that users' privacies remain intact, there is a growing trend towards system-level privacies for individuals.

Technology and Privacy

Tech companies like Apple, Facebook, Google, and others create large data from their users. A Cisco report forecasted an increase in IP traffic from approximately 37,075 GB per second in 2016 to 107,291 GB per second in 2021 (2016). In contrast, an updated estimate from Cisco and the World Bank Group estimates 150,000 GB per second of data by 2022 (2019; 2021). Of course, the initial forecasts could not have predicted the COVID-19 pandemic, which prompted an exponential increase in internet traffic. Along with data showing that 80% of adults in the United States use some form of social media several times throughout the day, it is easy to see how much data individuals generate daily (Auxier & Anderson, 2021).

The amount of data that individuals generate is important for tech companies. Companies use this data to run and sell advertisements on their sites. Because social media is free to use, companies make most of their profits from advertising revenue (Leetaru, 2018). Mark Zuckerberg, founder and CEO of Facebook, responded to Senator Orrin Hatch's question of how tech companies make money with, "Senator, we run ads" (CSPAN, 2018). Senator Hatch's lack of understanding of how companies sell users' data is indicative of how little the public knows (past and present) about how major tech companies operate. After all, these tech companies are part of a billion-dollar industry that commodifies user data in exchange for services. But how did we get to this point?

In the relatively early days of internet society, there were few protections in place that would ensure a user's privacy. While European countries enabled data protection statutes before 2000 (Sian, 2012; Solove, 2006), the first and most lasting piece of legislation in the United States is the Digital Millennium Copyright Act (DMCA) of 1998. While the DMCA protects internet service providers from copyright infringement, individual internet subscribers could still be tied to requests for information like copyright infringement (Katyal, 2004; Penney, 2019). Even with the ability to connect IP addresses to people, there are errors. As one family in Kansas found out, 600 million IP addresses were associated with their rented farm address (Farivar, 2016), prompting repeated queries from law enforcement and other officials.

Perhaps one of the largest discoveries of online privacy infringement happened in 2013 when former NSA analyst Edward Snowden revealed the government-run PRISM program that allowed unfettered government surveillance of corporations and private citizens (Farrell & Newman, 2019; Lucas, 2014; Macnish, 2018). PRISM was a direct result of the 2001 USA PATRIOT Act and the 2007 Protect America Act, laws that allowed for a massive overreach of how much the government could use digital tools to invade the daily lives of people.

The Patriot Act and the Protect America Act affect users through the government's interpretation of data and its relation to the US border. Data exists on servers, which are computer hardware containing the data that make up the ones and zeros of the internet. Additionally, servers are often located outside of the United States where they may be cheaper to build and where the energy required to cool and maintain the equipment is more cost-effective. If you download a photo you find on the internet and share it with friends, the data for that photo could exist anywhere from California to Maine, or in countries in Europe, South America, or Asia. The way the Patriot Act and the Protect America Act have been interpreted is that any digital data crossing the US border is subject to surveillance. This specific example of privacy intrusion by the government has been done in the name of national security. In the late 2000s/early 2010s, the United States experienced major technological events like Edward Snowden's data leak. Consequently, Congress passed the Personal Data Privacy and Security Act of 2009, increasing punishment for identity theft and other such privacy and security breaches. Otherwise, data privacy rights were largely under the purview of individual states.

Not until the passage of the General Data Protection Regulation (GDPR) in 2016 and the California Consumer Privacy Act (CCPA) of 2018 would there be major steps toward online privacy. The GDPR is a European Union law regulating data protection and privacy; the CCPA gives individuals more control over their data and how companies can use that data. With so many tech companies located in California and a significant portion of consumers/customers in Europe, these

statutes have helped establish de facto standards of online privacy and data privacy (Barrett, 2019; *California Consumer Privacy Act* (CCPA), 2018; Fazlioglu, 2020; Rakoski, 2021; Regulation 2016/679).

Another event that necessitated greater privacy regulations occurred in 2017 with the Cambridge Analytica (CA)-Facebook incident. This incident demonstrated the need for the increased privacy regulations that the CCPA provided. Cambridge Analytica (CA) was a company that provided resources and services for political campaigns around the globe. However, Facebook gave CA unrestricted access to users' data and other personally identifiable information (Isaak & Hanna, 2018; Shipman & Marshall, 2020). The ability to micro-target ads and information to individuals only became possible with the data that users unknowingly gave to private companies. What made the incident so egregious was that Cambridge Analytica used Facebook users' information without letting them know *the purpose* of their information collection, and CA has since been tied to political interference in the 2014 US Midterm elections, the 2016 Brexit referendum, and the 2016 US Presidential election (Hinds et al., 2020; Richterich, 2018; ur Rehman, 2019). After all, it is one thing to agree to limited information in exchange for free services; it is another to allow companies enough individual information to alter entire elections.

Data brokers add another layer of data privacy intrusions to existing privacy concerns. While the idea of large data sets based on metadata or non-identifiable information seems safe to use, the practical reality is that individuals are identifiable. Data brokers and others in the practice of trading people's information can use the data that they buy, sell, and gather through targeted ads (e.g., Facebook) for election misinformation (Otto et al., 2007; Rostow, 2017). Moreover, the longevity of digital data prevents the right to be forgotten in many cases in the United States. While Europe and the European Union may allow individuals to ask Google and other online platforms to "forget" (i.e., remove) certain information about themselves, the United States does not enjoy those same privacy protections (Gajda, 2018; Rosen, 2011; Tsesis, 2014). Additionally, "public figures" exist under the "right to know" provisions of information (Shackelford, 2012; Yanisky-Ravid & Lahav, n.d.).

Discussion

So how do discussions on data privacy, libraries in higher education, and digital literacy begin? It's complicated. There needs to be legislation and general best practices capable of protecting individuals' data privacy, and there also needs to be accountability and real consequences for those who misuse and abuse individuals' rights to privacy. Ultimately, this is a complex issue without a single solution.

One way of addressing the complexities of data privacy is to start with individuals and provide them with the education to be information-literate citizens. Information literacy is not only an important part of higher education in developing critical thinking and problem-solving skills, but it also prepares students to be a part of an information-rich society. Never has there been more information circulated and generated on a regular basis, and data and information circulation will only continue to increase exponentially in the future (Eisenberg et al., 2004; Koltay, 2011; Rockman, 2004; Ross et al., 2016). *Digital* information literacy is adding a layer of digital data and information to the existing scaffold of information literacy in a complex digital world (Jeffrey et al., 2011; Sparks, et al., 2016).

Libraries have been the entity in higher education charged with much of the information literacy pedagogy. From the humanities to the sciences and everywhere in between, the university or academic library remains at the core of the institution when it comes to information literacy (Hicks & Lloyd, 2021; Sample, 2020; Sparks, et al., 2016). With libraries being systems that understand the value of privacy and caution when it comes to innovations in information technologies, librarians tend to understand the theoretical ramifications of data privacy along with its practical applications. Librarians' professional experience and educational qualifications make them ideal candidates for teaching information literacy.

Higher educational institutions require librarians to have a master's degree, either an MLIS (Master of Library and Information Science) or some equivalent. Additionally, to be accredited by the American Library Association (2008), a master's program needs to meet several core competencies in research, technology, information resources, and other related domains. In addition, there are many specializations a person can focus on both as a core function for their work and for scholarship. Data management librarians, information literacy librarians, and instruction librarians are but a few of the different titles held by librarians who regularly deal with information literacy.

Libraries are not in the business of selling data (private or otherwise). Instead, libraries focus on keeping user data private, and there has always been a professional emphasis on supporting individual privacy. This exists within scholarly pedagogies emphasizing good data practices and the de-identification of individuals. While additional revenue streams are always welcome in the library given the rising cost of journal and database access, selling student data would be against traditions and practices in higher education libraries.

These libraries and librarians are a potential source for teaching digital information literacy, not only because of their establishment as an information and knowledge center at the university but also because they are already providing these types of literacy services and teaching. There are already many opportunities and resources for collaboration between librarians and the university. The Johns Hopkins Digital Literacy Resources guide, the University of British Columbia's Digital Tattoo project, Syracuse University's Center for Digital Literacy, and the University of Pennsylvania's Digital Literacy Fellows program are just some of the examples where libraries/librarians lead or collaborate to bring digital literacy to higher education. Additional digital literacy services performed by librarians include regular instruction and reference sessions that connect students and faculty with the library (Kocevar-Weidinger et al., 2019; Martzoukou & Sayyad Abdi, 2017; Meyers, et al., 2013). All these practical efforts are on top of the scholarship that librarians produce that look at historical, current, and future practices of digital literacies (Withorn et al., 2021).

What the average user needs to realize is that there are processes in place to protect their data. Even though it can be annoying to have to review privacy settings for websites or perform regular audits of what platforms have access to your email and Facebook data, a well-informed, data information literate person will know *why* these measures are in place and appreciate the effort it took to get here. Until there is a critical mass of people and companies who build information technologies and use them with data privacy in mind, education is another way to address the issue. One way to start that journey is to begin at the library with its librarians.

References

ALA Office for Intellectual Freedom. (2010). *Privacy and freedom of information in 21st-century libraries*. American Library Association.

Abbott, H. (2022). How data stewards make decisions to protect or disclose student information: Toward consistent criteria. *College & University*, 97(1), 2–9.

Allen, E. (2014, January 15). A *half century of library computing. Library of Congress Blog.* https://blogs.loc.gov/loc/2014/01/a-half-century-of-library-computing/

American Library Association. (2002). *Privacy: An interpretation of the library bill of rights* https://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy

American Library Association. (2008, June 10). *Core competences* https://www.ala.org/educationcareers/careers/corecomp/corecompetences

Arms, W. Y. (2012). The 1990s: The formative years of digital libraries. *Library Hi Tech*, 30(4), 579–591. https://doi.org/10.1108/07378831211285068

Association of College & Research Libraries. (2015, February 9). *Framework for information literacy for higher education.* https://www.ala.org/acrl/standards/ilframework

Auxier, B., & Anderson, M. (2021). *Social media use in 2021.* Pew Research Institute. https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/

Avram, H. D. (1975). *MARC; its history and implications*. Superintendent of Documents, U.S. Government Printing Office. http://eric.ed.gov/ERICWebPortal/detail?accno=ED127954

Barrett, C. (2019). Are the EU GDPR and the California CCPA becoming the de facto global standards for data privacy and protection? *The SciTech Lawyer*, 15(3), 24–29.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 35(4), 1017–1041. https://doi.org/10.2307/41409971

Brown, M., & Klein, C. (2020). Whose data? Which rights? Whose power? A policy discourse analysis of student privacy policy documents. *Journal of Higher Education*, 91(7), 1149–1178. https://doi.org/10.1080/00221546.2020.1770045

California Consumer Privacy Act (CCPA). (2018, October 15). State of California Department of Justice, Office of the Attorney General. https://oag.ca.gov/privacy/ccpa

Campbell, D. G., & Cowan, S. R. (2016). The paradox of privacy: Revisiting a core library value in an age of big data and linked data. *Library Trends*, 64(3), 429–511. http://dx.doi.org/10.1353/lib.2016.0006

Cisco. (2016). *Global –2021 forecast highlights.* Cisco. https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/Global_2021_Forecast_Highlights.pdf

Cisco. (2019). *Cisco visual networking index: Forecast and trends, 2017–2022.* Cisco. https://twiki.cern.ch/twiki/pub/HEPIX/TechwatchNetwork/HtwNetworkDocuments/white-paper-c11-741490.pdf

Cooke, L. (2018). Privacy, libraries and the era of big data. *IFLA Journal*, 44(3), 167–169. https://doi.org/10.1177/0340035218789601

CSPAN. (2018, April 10). *User Clip: Conversation between Mark Zuckeberg and Senator Orring Hatch—"Senator, we run ads"* [Video]. C-SPAN. https://www.c-span.org/video/?c4726758/user-clip-conversation-mark-zuckeberg-senator-orring-hatch-senator-run-ads

Dahl, M. (2009). The evolution of library discovery systems in the web environment. *OLA Quarterly*, 15(1), 5–9. https://doi.org/10.7710/1093-7374.1229

Digital Millennium Copyright Act, H.R. 2281, 105th Cong. (1998). https://www.congress.gov/bill/105th-congress/house-bill/2281

Eisenberg, M. B., Lowe, C. A., & Spitzer, K. L. (2004). *Information literacy: Essential skills for the information age*. ERIC.

Farivar, C. (2016, August 10). Kansas couple sues IP mapping firm for turning their life into a "digital hell." *Ars Technica.* https://arstechnica.com/tech-policy/2016/08/kansas-couple-sues-ip-mapping-firm-for-turning-their-life-into-a-digital-hell/

Farrell, H., & Newman, A. L. (2019). Of privacy and power: The transatlantic struggle over freedom and security. In *Of Privacy and Power*. Princeton University Press.

Fazlioglu, M. (2020). The United States and the EU's General Data Protection Regulation. In *Data Protection Around the World* (pp. 231–248). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-407-5_10

Gajda, A. (2018). Privacy, press, and the right to be forgotten in the United States. *Washington Law Review*, 93(1), 201-264. https://ssrn.com/abstract=3144077

Gardner, C. (2002). Fact or fiction: Privacy in American libraries. *Proceedings of the 12th Annual Conference on Computers, Freedom and Privacy*, 1–5. https://doi.org/10.1145/543482.543503

Giza, P. (2022). Automated discovery systems, part 1: Historical origins, main research programs, and methodological foundations. *Philosophy Compass*, 17(1). https://doi.org/10.1111/phc3.12800

Hess, A. N., 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

Hicks, A., & Lloyd, A. (2021). Deconstructing information literacy discourse: Peeling back the layers in higher education. *Journal of Librarianship and Information Science*, 53(4), 559–571. https://doi.org/10.1177/0961000620966027

Hinds, J., Williams, E. J., & Joinson, A. N. (2020). "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies*, 143, 102498. https://doi.org/10.1016/j.ijhcs.2020.102498

Inouye, T. M., & Vincent Agnello, J. D. (2015). Higher education industry consolidation: Where does it leave students? *Journal of Religion and Business Ethics*, 4(1), 1–14.

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer*, 51(8), 56–59. https://doi.org/10.1109/MC.2018.3191268

Jeffrey, L., Hegarty, B., Kelly, O., Penman, M., Coburn, D., & McDonald, J. (2011). Developing digital information literacy in higher education: Obstacles and supports. *Journal of Information Technology Education: Research*, 10(1), 383–413. http://dx.doi.org/10.28945/1532

Katyal, S. K. (2004). Privacy vs. Piracy. *Yale Journal of Law & Technology*, 7.

Kenyon, A. T., & Richardson, M. (2006). *New dimensions in privacy law: International and comparative perspectives*. University Press.

Klinefelter, A. (2007). Privacy and library public services: Or, I know what you read last summer. *Legal Reference Services Quarterly*, 26(1-2), 253–279. https://doi.org/10.1300/J113v26n01_13

Kocevar-Weidinger, E., Cox, E., Lenker, M., Pashkova-Balkenhol, T., & Kinman, V. (2019). On their own terms: First-year student interviews about everyday life research can help librarians flip the deficit script. *Reference Services Review*, 47(2), 169–192. https://doi.org/10.1108/RSR-02-2019-0007

Koltay, T. (2011). The media and the literacies: Media literacy, information literacy, digital literacy. *Media, Culture & Society*, 33(2), 211–221. https://doi.org/10.1177/0163443710393382

Leetaru, Kalev. (2018, December 15). *What does it mean for social media platforms to "sell" our data?* Forbes. https://www.forbes.com/sites/kalevleetaru/2018/12/15/what-does-it-mean-for-social-media-platforms-to-sell-our-data/?sh=54620a082d6c

Lambert, A. D., Parker, M., & Bashir, M. (2015). Library patron privacy in jeopardy an analysis of the privacy policies

of digital content vendors. Proceedings of the *Association for Information Science and Technology*, 52(1), 1–9. https://doi.org/10.1002/pra2.2015.145052010044

Lowenstein, H. (2016). The great wall of FERPA: Surmounting a law's barrier to assurance of learning. *The Journal of Legal Studies Education*, 33(1), 129–164. https://doi.org/10.1111/jlse.12037

Lucas, G. R. (2014). NSA Management Directive #424: Secrecy and privacy in the aftermath of Edward Snowden. *Ethics & International Affairs*, 28(1), 29–38. https://doi.org/10.1017/S0892679413000488

Macnish, K. (2018). Government surveillance and why defining privacy matters in a post-Snowden world. *Journal of Applied Philosophy*, 35(2), 417–432. https://doi.org/10.1111/japp.12219

Magi, T. J. (2010). A content analysis of library vendor privacy policies: Do they meet our standards? *College & Research Libraries*, 71(3), 254–272.

Martzoukou, K., & Sayyad Abdi, E. (2017). Towards an everyday life information literacy mind-set: A review of literature. *Journal of Documentation*, 73(4), 634–665. https://doi.org/10.1108/JD-07-2016-0094

Matz, C. (2008). Libraries and the USA PATRIOT Act: Values in conflict. *Journal of Library Administration*, 47(3–4), 69–87. https://doi.org/10.1080/01930820802186399

McKinnon, D., & Turp, C. (2022). Are library vendors doing enough to protect users? A content analysis of major ILS privacy policies. *The Journal of Academic Librarianship*, 48(2). https://doi.org/10.1016/j.acalib.2022.102505

Meyers, E. M., Erickson, I., & Small, R. V. (2013). Digital literacy and informal learning environments: An introduction. *Learning, Media and Technology*, 38(4), 355–367. https://doi.org/10.1080/17439884.2013.783597

Murray, P. E. (2001). Library Web proxy use survey results. *Information Technology & Libraries*, 20(4), 172.

Otto, P. N., Antón, A. I., & Baumer, D. L. (2007). The choicepoint dilemma: How data brokers should handle the privacy of personal information. *IEEE Security & Privacy*, 5(5), 15–23. https://doi.org/10.1109/MSP.2007.126

Oxford University Press. (n.d.). Privacy. In *OED Online*. Retrieved May 14, 2022, from http://www.oed.com/view/Entry/151596

Pachefsky, R. (1969). Survey of the card catalog in medical libraries*. *Bulletin of the Medical Library Association*, 57(1), 10–20.

Penney, J. W. (2019). Privacy and legal automation: The DMCA as a case study. *Stanford Technology Law Review*, 22, 412–486.

Pekala, S. (2017). Privacy and user experience in 21st century library discovery. *Information Technology and Libraries*, 36(2), 48–58. https://doi.org/10.6017/ital.v36i2.9817

Rakoski, R. L. (2021). Navigating global privacy regulations. *Benefits Magazine*, 58(3), 50–56.

Regulation 2016/679 *General Data Protection Regulation (GDPR)*. Retrieved May 15, 2022, from https://gdpr-info.eu/

Richterich, A. (2018). How data-driven research fueled the Cambridge Analytica controversy. *Partecipazione e Conflitto*, 11(2), 528–543. https://doi.org/10.1285/i20356609v11i2p528

Rockman, I. F. (2004). *Integrating information literacy into the higher education curriculum: Practical models for transformation*. Jossey-Bass.

Rosen, J. (2011). The right to be forgotten. *Stanford Law Review Online*, 64, 88–92.

Ross, M., Perkins, H., & Bodey, K. (2016). Academic motivation and information literacy self-efficacy: The importance of a simple desire to know. *Library & Information Science Research*, 38(1), 2–9. https://doi.org/10.1016/j.lisr.2016.01.002

Rostow, T. (2017). What happens when an acquaintance buys your data: A new privacy harm in the age of data brokers. *Yale Journal on Regulations*, 34(2), 667–707.

Rotenberg, M., Scott, J., & Horwitz, J. (2015). *Privacy in the modern age: The search for solutions*. The New Press.

Rubel, A. (2014). Libraries, electronic resources, and privacy: The case for positive intellectual freedom. *The Library Quarterly*, 84(2), 183–208. https://doi.org/10.1086/675331

Sample, A. (2020). Historical development of definitions of information literacy: A literature review of selected resources. *The Journal of Academic Librarianship*, 46(2), 102116. https://doi.org/10.1016/j.acalib.2020.102116

Schrameyer, A. R., Graves, T. M., Hua, D. M., & Brandt, N. C. (2016). Online student collaboration and FERPA considerations. *TechTrends*, 60(6), 540–548. https://doi.org/10.1007/s11528-016-0117-5

Scott, W. R. (2007). *Organizations and organizing: Rational, natural, and open system perspectives* (1st ed.). Pearson Prentice Hall.

Shabtai, A., Morad, I., Kolman, E., Eran, E., Vaystikh, A., Gruss, E., Rokach, L., & Elovici, Y. (2013). IP2User — Identifying the username of an IP address in network-related events. 2013 *IEEE International Congress on Big Data*, 435–436. https://doi.org/10.1109/BigData.Congress.2013.73

Shackelford, S. J. (2012). Fragile merchandise: A comparative analysis of the privacy rights for public figures. *American Business Law Journal*, 49(1), 125–208. https://doi.org/10.1111/j.1744-1714.2011.01129.x

Shipman, F., & Marshall, C. (2020, April). Ownership, privacy, and control in the wake of Cambridge Analytica. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. CHI Conference 2020, Honolulu HI USA. https://doi.org/10.1145/3313831.3376662

Sian, R. (2012). Origins and historical context of data protection law. In Eduardo Ustaran (Ed.), *European privacy: Law and practice for data protection professionals*. International Association of Privacy Professionals.

Sloot, B. van der, & Groot, A. de. (2018). *The handbook of privacy studies: An interdisciplinary introduction*. University Press. https://doi.org/10.1515/9789048540136

Solove, D. J. (2006). A brief history of information privacy law (SSRN Scholarly Paper No. 914271). *Social Science Research Network*. https://papers.ssrn.com/abstract=914271

Sparks, J. R., Katz, I. R., & Beile, P. M. (2016). Assessing digital information literacy in higher education: A review of existing frameworks and assessments with recommendations for next-generation assessment. *ETS Research Report Series*, 2016(2), 1–33. https://doi.org/10.1002/ets2.12118

Spilka, J. (2022). 377 Book challenges tracked by ALA in 2019–and the problem is growing: Book banning and its adverse effects on students. *Knowledge Quest*, 50(5), 30–33.

Starr, J. (2004). Libraries and national security: An historical review. *First Monday*, 9(12). https://doi.org/10.5210/fm.v9i12.1198

Surace, C. J. (1970). *Library circulation systems–an overview*. RAND Corporation.

Syracuse University. (n.d.). *Center for Digital Literacy*. https://www.digital-literacy.syr.edu/

Tsesis, A. (2014). The right to erasure: Privacy, data brokers, and the indefinite retention of data. *Wake Forest L. Rev.*, 49, 433–484.

University of British Columbia. (n.d.). *Digital Tattoo*. https://digitaltattoo.ubc.ca/

University of Pennsylvania. (n.d.). *Hoesley Digital Literacy Fellows Program*. https://www.curf.upenn.edu/content/hoesley-digital-literacy-fellows-program

ur Rehman, I. (2019). Facebook-Cambridge Analytica data harvesting: What you need to know. *Library Philosophy and Practice*. 2497.

Wang, Y., Liu, T., Tan, Q., Shi, J., & Guo, L. (2016). Identifying users across different sites using usernames. *Procedia Computer Science*, 80, 376–385. https://doi.org/10.1016/j.procs.2016.05.336

Wells, D. (2020). *Online public access catalogues and library discovery systems* [Text]. https://www.isko.org/cyclo/opac

Welsh Medical Library. (n.d.). *Digital and Information Literacy*. Johns Hopkins University. https://browse.welch.jhmi.edu/teaching-learning-resources/digital-information-literacy

Withorn, T., Eslami, J., Lee, H., Clarke, M., Gardner, C. C., Springfield, C., Ospina, D., Andora, A., Castañeda, A., Mitchell, A., Kimmitt, J. M., Vermeer, W., & Haas, A. (2021). Library instruction and information literacy 2020. *Reference Services Review*, 49(3/4), 329–418. https://doi.org/10.1108/RSR-07-2021-0046

Yanisky-Ravid, S., & Lahav, B. Z. (n.d.). Public interest vs. private lives—Affording public figures privacy in the digital era: The three principle filtering model. *University of Pennsylvania Journal of Constitutional Law*, 19(5). https://ssrn.com/abstract=2931864

Yoose, B. (2017). Balancing privacy and strategic planning needs: A case study in de-identification of patron data. *Journal of Intellectual Freedom & Privacy*, 2(1), 15–22. https://doi.org/10.5860/jifp.v2i1.6250