

Internet filters in Canadian libraries: Impact on intellectual freedom & social responsibility

Kate Schulz

¹*School of Library and Information Studies, University of Alberta, Email: keschulz@ualberta.ca*

To Cite:

Schulz, K. (2020). Internet filters in Canadian libraries. *Pathfinder: A Canadian Journal for Information Science Students and Early Career Professionals*, 1(2), 36-50. <https://doi.org/10.29173/pathfinder23>

Abstract

Internet filters are a method to block access to web content (Lawrence & Fry, 2016). Instantaneously, the word 'blocks' causes advocates of intellectual freedom to stand at attention. Intellectual freedom is one of the core values of librarianship which guide the decisions librarians make, as outlined within the American Library Association's (ALA) *Code of Ethics* (1939/2008). The ALA's *Library Bill of Rights* (1939/2019) states that, "a person's right to use a library should not be denied or abridged because of origin, age, background, or views" (para. IV). More specific to the topic at hand: "the use of Internet filters to block constitutionally protected speech ... compromises First Amendment freedoms and the core values of librarianship" (ALA, n.d., para. 1). This paper will investigate and discuss the function of and methodology behind internet filters, with specific attention to their application in Canada. Following a general overview, a discussion follows of what library professionals in public and school libraries should do to uphold and protect intellectual freedom.

Keywords: Internet filters, Canadian libraries, intellectual freedom, school libraries, public libraries

Intellectual freedom can be boiled down to the ability for all individuals to have free, unobstructed access to all forms of information and the beliefs contained within that information (Jensen, 2004). Alfino (2014) further emphasizes its importance and states that intellectual freedom "places fundamental value on the autonomy of the individual to hold and express beliefs without fear of political or social punishment" (p. 9). Therefore, it is understandable why internet filters can be viewed as an attack on this right. Historically, the filtering of materials – completed by state actors – was explicit, as physical media was removed from the preview of the general public. Examples of this form of censorship are events such as Die Säuberung in the 1930s: the Nazi

government book burning events, and the Cultural Revolution in China under Chairman Mao Zedong (United States Holocaust Memorial Museum, n.d.; Hu, 2017). In the age of internet communication, the filtering of content is covert; a user may not even realize they have been subject to filtering, as may be the case with location-based search results using search engines such as Google (Franti, Tabarcea, Kuittinen, & Hautamaki, 2010).

This paper will investigate the application of internet filters by state or government authorities and what they mean for library professionals in relation to upholding and protecting intellectual freedom. In section 1, an overarching overview of internet filters is introduced; their function and method of implementation is discussed from a generalized, global perspective. Section 2 narrows the scope and description of internet filtering to their manifestation in Canada. Next, section 3 looks at the effects of internet filters in Canadian public and school libraries. In addition, this section also discusses our professional duty as librarians and what we can do to ensure that the right to intellectual freedom is protected for our patrons. Finally, section 4 summarizes the findings of this paper and suggests an area for future research.

A General Overview of Internet Filters

Before delving into the topic of internet filters, a basic definition of what they are is necessary. Lawrence and Fry (2016) review internet filtering software and explain that its purpose is to:

Restrict users' access to web content. There are varied methods for blocking content to meet this end. For instance, filtering software might limit access on the basis of keywords or text strings, scanned pixels, third-party site ratings, or some other information source. (p. 404)

Filtering software was first developed in the mid-1990s in response to mounting concern and anxiety regarding potentially controversial topics on the internet, and the perceived vulnerability of minors who may gain access to it (Lawrence & Fry, 2016). Additionally, the term 'filters' may be used to describe "algorithmic personalization" (Peterson, Oltmann, & Knox, 2017, p. 4584); this relates to one's social media feed, for example, as the information presented there is curated for each user depending on their activity, beliefs, and interests.

When a government decides to filter the internet, “laws and technical measures [are put in place] to block their citizens from accessing or publishing information online” (Zittrain & Palfrey, 2008, p. 32). Zittrain and Palfrey (2008) further explain that these laws are generally “extensions of pre-existing media or telecommunications regulatory regimes” (p. 32), but may sometimes be “Internet-specific statutes and regulations” (p. 32). The United States Congress passed the Children’s Internet Protection Act (CIPA) in 2000; this Act “required American public schools and libraries seeking federal funding to implement [filtering technology]” (Peterson et al., 2017, p. 4587). CIPA was challenged by a coalition led by the ALA, which argued that it “imposed an unconstitutional condition on public institutions to block access to constitutionally protected speech” (Peterson et al., 2017, p. 4587). However, the Supreme Court ultimately upheld CIPA in 2003 (now called COPPA: The Children’s Online Privacy Protection Act) and, since then, all American public schools, as well as most public libraries, have implemented technology to filter content (Peterson et al., 2017). At present, Canada does not have an equivalent federal law to protect children’s online privacy (Lawton, as cited in Campbell, 2014, para. 5).

A nation may block access to content based on the political or religious message it expresses, or even the social connotations it has (Zittrain & Palfrey, 2008). China, for example, has employed varying degrees of content restrictions which “disallow citizens from publishing or accessing certain content online” (Zittrain & Palfrey, 2008, p. 33). France and Germany both have a requirement wherein the government body limits internet access to certain materials, including “a ban on ‘propaganda against the democratic constitutional order’” (Zittrain & Palfrey, 2008, p. 33). Nations may also block sites that host content that infringes on intellectual property rights. The United Kingdom arguably has “one of the most developed and advanced regimes in Europe” in this regard (Alexander & Hepburn, 2019, para. 1). The process has been reviewed and streamlined so that the court process can grant right-holders relief more efficiently (Alexander & Hepburn, 2019).

How do nations go about filtering the internet? From the studies completed by Zittrain and Palfrey (2008), they found that most countries rely on “preidentification and categorization of undesirable Web sites” (p. 36). This manual process takes time, and

they state that the evolution and growth of Web 2.0 makes this process more difficult “as citizens have the ability to publish online content on the fly and to syndicate that content for free” (Zittrain & Palfrey, 2008, p. 36). Web 2.0 is “the stage of the Web that allows users to connect through interactive technology [(i.e., social media websites)]” (Mazzei, 2019, Definition of Web 2.0 section, para. 1). The manual process involves identifying URLs that lead to undesirable content and disabling access to those sites (Zittrain & Palfrey, 2008). They highlight that this system – besides being labourious – is not perfect; for example, based on URL alone, “blogging or generic free Web-hosting sites like www.geocities.com” (p. 36), may be blocked. However, this action blocks all content: ‘good’ or ‘bad,’ as the URL doesn’t provide information about the content on the sites. While filtering software has become more context-sensitive over time, both under- and over-blocking of content can occur (Lawrence & Fry, 2016). Commercial software programs are available to assist with implementing block lists, such as *K9 Web Protection* (Peterson et al., 2017). These types of programs come with extensive, categorized lists that allow countries to block content at a categorical level (Zittrain & Palfrey, 2008). However, this can lead to over-blocking since the commercial filters have nations decide between “allowing or blocking all URLs within a category” (Zittrain & Palfrey, 2008, p. 39). Overall, at least at this time, there does not seem to be an easy way to effectively identify and categorize websites for the purpose of filtering.

Internet filtering is not necessarily viewed in a negative light in all instances; for example, internet filtering may be a method to uphold the law. Zittrain and Palfrey (2008) cite the example of child pornography; no one would protest a state’s right to block such content. “The need for states to be able to exercise some measure of control online is broadly accepted” (Zittrain & Palfrey, 2008, p. 44). Most people would also not raise issue with the state having some form of control in order to prevent online fraud or other crime, as well as to protect intellectual property (Zittrain & Palfrey, 2008). Contemporary justification of online censorship and surveillance is that it’s a method to “counteract international terrorism” (Zittrain & Palfrey, 2008, p. 45); that is: “Internet filtering and surveillance, in an environment where the Internet is considered a form of territory alongside land or sea or air, are an expression of the unalterable right of a state to ensure its national security” (Zittrain & Palfrey, 2008, p. 45).

This becomes an issue for many when internet filtering and surveillance may encroach upon individual civil liberties (Zittrain & Palfrey, 2008). Online surveillance is the monitoring of online activity by an overseeing government body (Zittrain & Palfrey, 2008). It is an individual's right to freely express their opinions: filtering and surveillance in the name of defending national security may be seen as an attack on one's "basic rights of *freedom of expression and individual privacy* [emphasis added]" (Zittrain & Palfrey, 2008, p. 49). Individuals are sharing more personal data and information online than ever before. Social media may be said to be largely responsible for this increase. Mon (2015) affirms this with her statement that "Web 2.0 media creates opportunities for social participation and contribution" (p. 1). In order to achieve these social aspects, users have increasingly shared personal data and aspects of their lives online. The primary critique of internet filtering – one that aligns with our professional duty as librarians:

Boils down to a belief in the value of a relatively open information environment because of the likelihood that it can lead to a beneficial combination of greater access to information, more transparency, better governance, and faster economic growth. ... The internet can give rise to a more empowered, productive citizenry. (Zittrain & Palfrey, 2008, p. 51)

With this stated critique in mind, I will now move on to looking at internet filters in Canada, both generally and with respect to libraries, and what they mean for our profession.

Internet Filters in Canada

Internet filters in Canada are far less widespread and encompassing compared to other countries in the world; however, this does not mean that the internet is unregulated in Canada (O'Keefe, Palfrey, & Seltzer, 2008). In Canada, O'Keefe et al. (2008) explain that content is restricted via legal and technical regulations in certain environments (e.g., school libraries); further, publishing hate speech is also restricted in Canada. O'Keefe et al. state that internet filtering has primarily been through "government-facilitated industry self-regulation" (p. 226). Additionally, "with the exception of child pornography, ... content restrictions tend to rely more on the removal of content [rather] than blocking: ... rely[ing] upon the involvement of private parties"

(O’Keefe et al., 2008, p. 226). O’Keefe et al. outline four areas in which internet filtering occurs in Canada: 1) regulation of obscene and explicit content, 2) defamation, 3) copyright, and 4) national/computer security; I will now provide a brief overview of their research findings in these areas.

With respect to sexually explicit content, Canada, compared to its neighbour to the south, has tended to act more conservatively in its approach (O’Keefe et al., 2008). O’Keefe et al. (2008) describe how Canadian legislators have made revisions to “existing obscenity provisions to encompass online offenses” (p. 227), rather than pursuing broader definitions and mandates. One such example is the passing of the Criminal Law Amendment Act of 2001, which:

Established online acts of distributing and accessing child pornography and luring a child as crimes. The Criminal Code mandates a system for judicial review of material (including online material) alleged to be child pornography. It does not, however, require [Internet Service Providers (ISPs)] to judge the legality of content posted on their servers ... [However,] if a judge determines that the material in question is illegal, ISPs may be required to take it down and to give information to the court to help in the identification and location of the person who posted it. (O’Keefe et al, 2008, p. 227)

Important to note is that, since both accessing and making child pornography accessible are illegal in Canada, this instance of internet filtering “does not infringe on rights of access or speech afforded by the Canadian Charter of Rights and Freedoms” (O’Keefe et al., 2008, p. 228).

In 2006, in partnership with Cybertip.ca, Canada’s largest ISPs launched Project Cleanfeed Canada, which is intended to protect their customers from “inadvertently visiting foreign Web sites that contain images of children being sexually abused and that are beyond the jurisdiction of Canadian legal authorities” (OpenNet Initiative, 2010, p. 375). The program is voluntary and blocking is left to the discretion of the ISPs; SaskTel, Bell Canada, and Telus all claim to only block specific URLs, not IP addresses, “in an attempt to avoid overblocking” (OpenNet Initiative, 2010, p. 375). Over-blocking would likely result in significant public outcry, as it may be viewed as ‘a

step too far' and infringe on Canadians' rights. OpenNet Initiative (2010) also highlights that this could be illegal under the Telecommunications Act.

Defamation is the "publication of an untrue statement about a person that tends to lower his reputation in the opinion of right-thinking members of the community or to make them shun or avoid him" (Law, 2018, Defamation section, para. 1). Legal liability constrains publishers of content on the internet and some ISPs (O'Keefe et al., 2008). This can result in a "chilling effect' on lawful online content and conduct and can threaten the anonymity of users" (O'Keefe et al., 2008, p. 230). While ISPs in the United States are provided with greater protection with respect to liability, this is not the case for Canadian providers and they "may be compelled to take down allegedly defamatory content (e.g., postings to message boards) under threat of suit" (O'Keefe et al., 2008, p. 230).

As with other areas when compared to the United States, Canada has been slower to evolve the law for issues arising from copyright (O'Keefe et al., 2008). O'Keefe et al. (2008) cite an example from 2004 of the *Interim Report on Copyright Reform*, which "proposed a notice-and-takedown policy ... under which Canadian service providers would be compelled to remove content immediately upon receiving notice of an alleged infringement from a professed copyright holder" (p. 231). This report received a lot of scrutiny and negative reaction from the public (O'Keefe, 2008). Since publishing their research, Canada has since passed and received Royal Assent for Bill C-11 in June of 2012, which is otherwise known as the *Copyright Modernization Act*. This Act states that, upon receiving notice of a claimed infringement, adhering to section 41.26(1)(a), the ISP shall forward the notice to the party in possible breach and retain records on the identity of that individual, as per section 41.26(1)(b) for the claimant to use if they choose to move forward with legal proceedings (Copyright Act, 1985).

The primary driver behind state-mandated limitations in Canada is security concerns; namely, national and computer security (O'Keefe et al., 2008, p. 232). This concern has resulted more in online surveillance rather than content filtering (O'Keefe et al., 2008). While related, internet filtering and online surveillance are different; surveillance can be understood as the monitoring and gathering of information about usage, while filtering may take that information in order to create filters to block access

(Stalla-Bourdillon, 2013). Even the *perception* of online surveillance is enough to make individuals pause before publishing or accessing certain content, particularly if it may be viewed as going against societal norms. O’Keefe et al. (2008) state that, in Canada, online surveillance is undertaken by the National Defense’s group, Communications Security Establishment (CSE), which works closely with the United States. Interestingly, “although bound by Canadian laws and prohibited from eavesdropping on solely domestic Canadian communications without explicit ministerial approval, the CSE’s activities are highly secret and oversight is minimal” (O’Keefe et al., 2008, p. 232).

To assist in computer security, particularly against spam, Canada assembled the National Task Force on Spam in 2005 to study the issue, which concluded that legislation should be put in place to limit spam from reaching computers (O’Keefe et al., 2008). As a result, Canada’s Anti-Spam Legislation (CASL) came into effect in 2014 to “reinforce best practices in email marketing and combat spam and related issues. These issues include identity theft, phishing and the spread of malicious software, such as viruses, worms and trojans (malware)” (Government of Canada, 2019, About CASL section, para. 1). This legislation has resulted in Canadians receiving less spam – “one study showed that within a year of the legislation being introduced, there was a 37% decrease in Canadian-based spam and 29% less email (spam or legitimate) in Canadians’ in-boxes” (Government of Canada, 2019, About CASL section, para. 4). However, while it may be perceived as ‘spam’ by the majority, some individuals may argue that they should retain the right to make their own choice about what they receive, without government oversight.

Overall, the Government of Canada has “experienced significant resistance to their content restriction policies” (O’Keefe et al., 2008, p. 233); therefore, internet filtering is fairly limited in this country. The areas that internet filtering apply to relate to law-keeping practices: the regulation of explicit content, defamation cases, copyright issues, and national/computer security. With their possible connection to upkeeping law and order, internet filters may be viewed differently with respect to intellectual freedom. However, in the realm of public and school libraries, does this add another layer of complexity as we consider how to protect ‘vulnerable minors?’ Therefore, I now turn to a

discussion on internet filtering in Canadian public and school libraries, as well as what our duty is as librarians in protecting intellectual freedom.

Internet Filters in Canadian Public and School Libraries: Our Duty as Librarians

Library professionals have always been advocates for intellectual freedom. Cooper (2010) argues that “by allowing individuals to have intellectual freedom, libraries help their users to develop information access skills ... [which] promotes responsible democratic citizenship” (p. 219). This relates to the social responsibility of libraries; Tise (2011) remarks that “libraries have always been – and will continue in that vein to be – that societal institution that propagates democracy and growth and development” (para. 1). Libraries “must use available technologies to provide innovative information services ... [and] interrogate future scenarios and challenges” against intellectual freedom (Tise, 2011, para. 3). For librarians, access means making “unbiased materials and services physically available in a structure organized for easy consumption, and hope for their use and utility” (Barniskis, 2016, p. 106). As makerspaces become more widespread, their role in intellectual freedom could be said to involve “ensuring equitable access to not only informational media, but also tools, spaces, and social networks that support knowledge, as well as facilitating users’ knowledge creation” (Barniskis, 2016, p. 103).

In general, society believes that minors should be protected against ‘bad’ and/or ‘harmful’ information. Evidence of this belief in action was discussed earlier through the example of the United States Congress enacting CIPA/COPPA (Peterson et al., 2017). This belief is also evidenced through assigning ratings to programming to indicate its intended audience (e.g., G, PG, or 18+) (Canadian Broadcast Standards Council, n.d.). School and public libraries often come up against unique challenges when it comes to intellectual freedom and censorship (Cooper, 2010). However, the ALA’s *Library Bill of Rights* (1939/2019) states: “a person’s right to use a library should not be denied or abridged because of origin, age, background, or views” (para. IV). Internet filters are seen as “antithetical to the mission of the library to provide free and open access to *all* [emphasis added] information” (Houghton-Jan, 2010, p. 40). Therefore, it becomes necessary for librarians to “provide students [(or children, in general)] with free access to information while also heeding to laws restricting what children can access and

respecting the concerns of parents” (Cooper, 2010, p. 221). Cooper (2010) suggests the following guideline for school librarians: “consider the suitability of materials in their collection based on age-appropriateness rather than on other agendas” (p. 221); personal or otherwise. In addition, Cooper emphasizes that they should work to build collections that represent all views and types of people, work with parents to educate them on library practices, and teach students socially responsible information access skills. Cooper’s suggestions can easily be extended to librarians in public libraries for patrons of the general population. More in line with this paper’s discussion of internet filters, Cooper also notes that “*acceptable use policies* [emphasis added] can alleviate some of the restrictions that arise because of laws requiring schools [or public libraries] to use filters to protect children from harmful sites on the Internet” (p. 222).

A principal concern with internet filtering is how commercial software programs classify and categorize content; “the automated classification processes and the whitelists and blacklists that filtering software companies develop are ferociously protected and never made publicly available to their customers” (Houghton-Jan, 2010, p. 42). Houghton-Jan (2010) articulates the following points as the issues libraries should consider before implementing, or re-assessing the use of, internet filters: “data collection, library privacy policies, confidentiality of information needs, and alternatives to filters” (p. 44). Stripling (2013) stresses that “individual librarians cannot afford to be complacent by assuming that [professional associations like the ALA] are ‘handling’ intellectual freedom issues” (p. 8). Each community must adopt policies and procedures and be diligent to update them as elements such as technology evolve in order to combat local intellectual freedom challenges (Stripling, 2013). Stripling discusses how, in recent years, libraries have gone through a shift in focus in how they advocate for their patrons with respect to intellectual freedom. Rather than maintaining a position of what the library can do, the role of the library should be to educate users; that is, “the intellectual-freedom question for librarians in user-centred libraries should be: ‘What must our libraries give patrons the freedom *to do* [emphasis added]?’” (p. 8).

This is where social responsibility manifests itself in the librarian’s duty to protect intellectual freedom. “If library patrons are going to be intellectually free, then librarians must teach them ... to be *socially responsible* [emphasis added] in the access and use

of information” (Stripling, 2013, p. 9). There are five areas of social responsibility that should be taught in order to empower patrons to exercise their right to intellectual freedom. These responsibilities are: “evaluating information; active searching for multiple perspectives; constructing one’s own ideas, opinions, and conclusions based on evidence; responsibly interacting with others; [and] monitoring one’s own online publishing and behavior” (Stripling, 2013, p. 9).

By teaching social responsibility, librarians can both provoke and support their users’ behavior in ways that guarantee their intellectual freedom to construct their own ideas. By sharing responsibility for intellectual freedom with their patrons, librarians strengthen the foundation of intellectual freedom for our society as a whole. (Stripling, 2013, p. 12)

As a final point of consideration, librarians do certainly have a professional responsibility to protect intellectual freedom and fight against censorship. However, Jensen (2004) argues that “parents should [also] take on their responsibility to teach their children what is appropriate. Internet filtering will not keep children from accessing or receiving inappropriate material” (p. 15). Parents have “both the right and the responsibility to choose whether to limit their children’s choices in the library” (Morgan, 2004, p. 6). Therefore, I believe that while we, as professionals, should uphold our responsibilities and duty, it is also our role to work *with* members of our communities – including parents – to promote intellectual freedom and educate the public on responsible use and access.

Conclusion

While not having nearly as many restrictions as some countries, internet filtering does still occur in Canada. Indeed, as highlighted by Zittrain and Palfrey (2008), the need to exercise some measure of restriction online is broadly accepted; particularly, in areas related to the distribution of unlawful content such as child pornography. In fact, this is one example of an area that Canada *does* implement the use of internet filters and content restrictions, with the other areas being cases of defamation, copyright issues, and matters of national/computer security (O’Keefe et al., 2008). Despite the existence of areas where filtering may not be questioned, there are many areas that do not fall under these categories. Therefore, library professionals play a key role in

upholding and protecting the patrons' right of intellectual freedom. Stripling (2013) argues that, "if library patrons are going to be intellectually free, then librarians must teach them ... to be socially responsible in the access and use of information" (p. 9). Protecting intellectual freedom cannot, and should not, be assumed to be handled by professional bodies such as the ALA alone. Each library, regardless of its type, must adopt policies and procedures and be diligent to update them as technology changes in order to combat local intellectual freedom challenges (Stripling, 2013). A more in-depth look and examination of social responsibility in relation to internet filters is worth future research. While the importance of teaching social responsibility was briefly touched upon in this paper, this is an aspect that I believe can be discussed more thoroughly on its own.

In conclusion, internet filters go against one of the core values of librarianship; however, through examination of their implementation in Canada, this paper has highlighted their 'appropriate' use, and provided guidance for librarians to protect intellectual freedom in today's ever-evolving technological world. While not always a simple topic to understand, I believe that keeping the value of educating patrons on responsible use and information access in mind will allow intellectual freedom to live on – even in the presence of internet filters.

Conflict of Interest Statement

None declared.

References

- Alexander, R., & Hepburn, K. (2019, February 22). *Building blocks – site blocking procedures, enhancements and the future development of the remedy* [Blog post]. <https://www.wiggin.co.uk/insight/building-blocks-site-blocking-procedures-enhancements-and-the-future-development-of-the-remedy>
- Alfino, M. (2014). Philosophies of intellectual freedom. In M. Alfino & L. Kolutsky (Eds.), *The Library Juice Press handbook of intellectual freedom: Concepts, cases, and theories* (pp. 9-40). Library Juice Press.
- American Library Association (ALA). (n.d.). *Filters and filtering*. <http://www.ala.org/advocacy/intfreedom/filtering>

- American Library Association (ALA). (2008). *Code of Ethics of the American Library Association* [PDF file]. <http://www.ala.org/advocacy/sites/ala.org/advocacy/files/content/proethics/codeofethics/Code%20of%20Ethics%20of%20the%20American%20Library%20Association.pdf> (Original document adopted in 1939).
- American Library Association (ALA). (2019). *Library Bill of Rights*. <http://www.ala.org/advocacy/intfreedom/librarybill> (Original document adopted in 1939).
- Barniskis, S. C. (2016). Access and express: Professional perspectives on public library makerspaces and intellectual freedom. *Public Library Quarterly*, 35(2), 103-125. 10.1080/01616846.2016.1198644
- Campbell, A. (2014, July 7). Online privacy protection for kids lagging in Canada. *The Star*. <https://www.thestar.com>
- Canadian Broadcast Standards Council. (n.d.). *Ratings classification for Canadian French-language broadcasters*. <http://www.cbsc.ca/tools/ratings-classifications/canadian-french-language-broadcasters>
- Cooper, J. L. (2010). Intellectual freedom and censorship in the library. *Community & Junior College Libraries*, 16(4), 218-224. doi:10.1080/02763915.2010.521016
- Copyright Act, R.S.C. 1985, c. C-42. <https://laws-lois.justice.gc.ca/eng/acts/c-42>
- Franti, P., Tabarcea, A., Kuittinen, J. & Hautamaki, V. (2010). Location-based search engine for multimedia phones. *Proceedings of the 2010 IEEE International Conference on Multimedia and Expo*, Suntec City, Singapore, July 19-23, 2010. New York, NY: IEEE.
- Government of Canada. (2019). Canada's Anti-Spam Legislation. <https://www.fightspam.gc.ca/eic/site/030.nsf/eng/home>
- Houghton-Jan, S. (2010). Internet filtering. In American Library Association (ALA) Office for Intellectual Freedom (OIF), J. Griffey, S. Houghton-Jan, & E. Neiburger, *Privacy and freedom of information in 21st century libraries (Library technology reports 46(8): Expert guides to library systems and services)* (pp. 40-54). American Library Association.
- Hu, A. (2017). *Mao and the Cultural Revolution*. Silkroad Press.
- Jensen, M. (2004). Internet filtering and its effects on intellectual freedom. *PNLA Quarterly*, 68(4), 13-15. <http://eds.a.ebscohost.com>

- Law, J. (Ed.). (2018). *A dictionary of law* (9th ed.) [eBook]. Oxford University Press.
- Lawrence, E., & Fry, R. J. (2016). Content blocking and the patron as situated knower: What would it take for an internet filter to work? *Library Quarterly*, *86*(4), 403-418. 10.1086/688030
- Mazzei, M. (2019). *Web 2.0*. Salem Press Encyclopedia of Science. <http://eds.a.ebscohost.com>
- Mon, L. (2015). The social media environment. In G. Marchionini (Ed.), *Synthesis lectures on information concepts, retrieval, and services* (pp. 1-18). Morgan & Claypool Publishers.
- Morgan, C. D. (2004). Internet filtering and individual choice. *OLA Quarterly*, *10*(4), 5-7. <http://eds.a.ebscohost.com>
- O'Keefe, K., Palfrey, J., & Seltzer, W. (2008). Internet filtering in the United States and Canada. In R. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access denied: The practice and policy of global Internet filtering* (pp. 226-234). MIT Press.
- OpenNet Initiative. (2010). *United States and Canada Overview* [PDF file]. <https://opennet.net/research/regions/namerica>
- Peterson, C., Oltmann, S. M., & Knox, E. J. M. (2017). The inconsistent work of web filters: Mapping information access in Alabama public schools and libraries. *International Journal of Communication*, *11*, 4583-4609. <http://eds.b.ebscohost.com>
- Stalla-Bourdillon, S. (2013). Online monitoring, filtering, blocking ... What is the difference? Where to draw the line? *Computer Law & Security Review*, *29*(6), 702-712. 10.1016/j.clsr.2013.09.006
- Stripling, B. K. (2013). Intellectual freedom: Moving beyond freedom from... to freedom to... *Library and Information Science Source*, *32*(1), 8-12. <http://eds.a.ebscohost.com>
- Tise, E. R. (2011). Forward. In D. Baker & W. Evans (Eds.), *Libraries and society: Role responsibility and future in an age of change* [eBook]. Chandos Publishing. <https://proquest.safaribooksonline.com>

United States Holocaust Memorial Museum. (n.d.). *Holocaust encyclopedia: Book burning*. <https://encyclopedia.ushmm.org/content/en/article/book-burning>

Zittrain, J., & Palfrey, J. (2008). Internet filtering: The politics and mechanisms of control. In R. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access denied: The practice and policy of global Internet filtering* (pp. 29-56). MA: MIT Press.