Digital Privacy for Minors

Concepts

The concept of digital privacy for minors, especially as it applies within a library context, is still evolving. While privacy for libraries’ patrons in general—or even adult patrons particularly—has been affirmed and reaffirmed throughout the last century, privacy for youth has been less clear of an issue. The advancement of digital technology, rather than clarify patrons’ needs and libraries’ visions, has only served to muddy the waters.

Vocabulary/Keywords

Privacy, Digital Privacy, Minors, Children, Teens, Libraries, COPPA (Children’s Online Privacy Protection Act), NSA (National Security Agency), Cookies, Databases, Vendors, HTTP, HTTPS

What Is Digital Privacy?

Digital advancements have altered the library landscape in many respects: they provide multiple avenues for information storage; they allow for more types of library interactions and therefore allow for more types of information to be collected; and they allow for a greater number of external organizations and third parties to collect and view this information. For example, whereas fifty years ago a query might have resulted in the manual pulling of some periodicals, the same research topic today will likely result in a search in electronic database. This database, in turn, may save a record of the search and the IP address of the searcher—and may share this information with other organizations. The Patriot Act, ongoing federal investigations, and large-scale data seizures by the NSA have raised further concerns.

Rights for Minors

Perhaps the greatest obstacle of developing a clear, consistent stance on minors’ digital privacy stems from lack of focus. Some libraries do not post any kind of privacy policy—at least not prominently—and many of the existing policies do not contain separate sections for the rights of minors. This may stem from disagreements about the nature of the issue. It is clear that children should be protected . . . but from whom? With adult patrons, this issue is very simple: the patrons are entities in their own right whose privacy must be safeguarded from libraries, who should not misuse data; and from government agencies, whose seizures of information, especially in the aftermath of Snowden, have generated much concern. In both cases, library privacy policies protect adults from external forces. With children, however, in addition to these external threats, some libraries try to protect them from internal forces as well, even from adults who know the child, including parents and teachers.

Official Stance on Children’s Privacy & Parental Concerns

There is no official agreement among libraries for reconciling children’s privacy with parents’ desire to know. Different libraries have adopted different policies, both within and without a digital context. Boston Public Library, for example, will not reveal to a parent the name of a
child’s missing book, even if the parent is financially responsible for that child. Similarly, San Francisco Public Library will not reveal minors’ borrowing history or items requested, even to their parents. At the other extreme is the New York Public Library, who will allow parents to know what items have been checked out by a child 11 or under, while the items of a minor 12 or older are only made available if they are overdue. In all three cases, these restrictions refer to physical materials. Privacy policies regarding minors specifically in digital contexts are—as far as I can tell—exclusively in the context of protecting children from external threats. In most cases, these policies take the form encouraging parents to warn the children not to share personal information, and reassuring them that the libraries will not be collecting personal information from children 13 and under. This is the case for New York Public Library, Chicago Public Library, and Bexar County Public Library in San Antonio. Bexar County’s privacy policy acknowledges that minors can still use the library’s services. However, the library also requires information as personal as an e-mail for a service as simple as a live chat session.

Bexar County Digital Library remembers my name and e-mail from a chat weeks before. The pop-up box with the chat options appears on every page. My computer will remember until I clear the cookies, but I have no way of knowing how long the library will store the data.

Presumably, the chat feature is geared toward teens and preteens.

The American Library Association has not voiced a clear position either. Their website includes a page of significant events affirming minors’ First Amendment Rights, including a court decision of 2001 that upheld children’s rights to play violent video games at an arcade without parental consent (ALA 2016c). Similarly, the ALA Library Bill of Rights recognizes patrons’ rights, regardless of age, and one of their interpretations is particularly specific: “The American Library Association opposes all attempts to restrict access . . . based on the age of library users” (ALA, 2016b). In their privacy toolkit, ALA addresses minors’ privacy from their parents: “Librarians should not breach a minor's confidentiality by giving out information readily available to the parent from the minor directly” (ALA 2016d). However, the ALA’s page of access for children to nonprint material affirms that parents “have the right and responsibility to restrict access of their children [and] to guide their own children’s reading and viewing” (ALA
2016a). This lack of clarity implies an uncertain stance as to the degree of parental involvement with their children’s library use. How much should parents know—or not know?

**Libraries Fight Back**

One serious drawback to libraries’ use of technology is that often, it is third-party vendors, contractors, and partners—and not libraries—who make the ultimate decisions regarding patron privacy. Even tasks as seemingly mundane as browsing the catalog become weightier matters. One blogger made one search on New York Public Library’s catalog, and he traced eight different companies his browser contacted in building the page. Privacy policies for these companies varied; some were nonexistent while others held such vague reassurances as “The information collection online is stored indefinitely and is used for various purposes” (Hellman, 2014). Many used cookies to track users. These companies are separate from NYPL and not subject to its policies. Some libraries, recognizing the dangers to privacy posed by third parties, have signed the Library Freedom Project’s Digital Library Privacy Pledge to use the encrypted HTTPS instead of HTTP. Library Freedom Project recognizes that “HTTPS is a privacy prerequisite, not a privacy solution” and views it as only the first step of the larger goal to build “a culture of library digital privacy” (n.d.). The organizations to sign the pledge include publishers and vendors as well as libraries (CLIR 2016).

New York Public Library’s catalog contacts eight different sites in building its results page. Some of these sites pass data on to other companies (Hellman, 2014).
An Uncertain Future

Bruce Schneier, CTO of Counterpane Internet Security, lamented online privacy breaches as violations of “an inherent human right [of] dignity and respect” (2006). Less than a decade later, Publishers Weekly wrote that libraries cannot guarantee absolute privacy and “shouldn’t want to” (Brantley, 2015). Brantley argues that people share information on social media all the time, and libraries need to assert their relevancy in the digital world by compiling patron data to offer personalized experiences; he argues this is “imperative” and suggests that tracking patron use, information, and even location to offer better service. He fails to address either the issue of minors’ data or government data seizures. Brantley’s ideas also may not be as accepted by patrons as he seems to think. In 2013, The Newsletter on Intellectual Freedom described Harvard University Library’s idea to post the titles of checked-out books on its Twitter feed: “It seemed harmless enough [but became] more provocative than library staffers imagined . . . Privacy concerns were raised [as people worried] that someone might somehow use other details to identify the borrowers” (“Libraries go digital,” 2013, p. 3). Other recent articles condemn libraries for a “disturbing trend” of not “giving privacy concerns their proper attention” (Gressel, 2014, p. 139). Gressel also argues that just because people share personal information on social media, “it does not mean that they do not care about privacy in general” (2014, p. 139). This touches on the delicate point that libraries may need to be even more concerned about privacy than patrons.

As for children’s privacy specifically, the laws vary from state to state, and libraries still approach the issue in different ways. One of the few federal initiatives to impact children’s digital privacy at libraries is the Children’s Online Privacy Protection Act, and even that affects websites directly, rather than libraries (ftc). In 2015, the National Information Standards Organization developed a set of principles on users’ digital privacy in library systems. The collaboration involved a steering committee of 9 and a core working group of 35 people; the resulting document is 11 pages long. Never once does it mention children, youths, parents, teens, or minors (NISO, 2015). As libraries continue to seek relevancy in a digital world, they may want to consider taking active measure to safeguard the digital privacy of their youngest patrons, and to document these measures as part of their privacy policies. Affirming children’s
need for digital privacy is a necessary step, and developing separate policies for minors or for
digital contexts may also help further their cause. Digital concerns over safety for minors are not
going away—nor should they. Now is the time for libraries to take stock, and to address their
concerns in tangible, written form. Now is the time for minors’ privacy rights to be given its
place in the professional literature.
References


