OLA Quarterly

Privacy and Confidentiality

Winter 2022 Vol 27 • No 1

OLAQ

OLA Quarterly
Winter 2022
Vol 27 • No 1

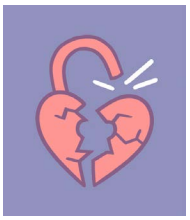
Oregon Library Association
http://www.olaweb.org
ISSN 1093-7374

The *OLA Quarterly* is an official publication of the Oregon Library Association. Please refer questions and input regarding the *Quarterly* to:

OLA Quarterly Editor-in-Chief:
Kate Lasky
olaq@olaweb.org

Copyeditor
Teresa Stover
Stover Writing Services
teresa@stoverwriting.com

Graphic Production:
Julie Weiss
Tobias Weiss Design
julie@tobiasweissdesign.com



Privacy and Confidentiality

From the Guest Editors

Ellie Avis (she/her) is the Collection Manager at Multnomah County Library. She is a member of the OLA Intellectual Freedom Committee and Tech Services Roundtable, and has been part of the Library Freedom Project since 2019. She holds a Master's Degree in City Planning from UC Berkeley and is currently working on her MLIS. In her free time, Ellie enjoys making and breaking things, DIY music, and riding her bike. Contact her at elliea@multcolib.org.

Kelly McElroy (she/her) is the Student Engagement and Community Outreach Librarian and an Associate Professor at Oregon State University. She has been a member of the Library Freedom Project since 2018. Kelly loves to get people talking about things that matter, whether as a facilitator for Oregon Humanities' Conversation Project or as an officer for her union, United Academics OSU. Contact her at kelly.mcelroy@oregonstate.edu or find her on Twitter at @kellymce.

Protecting patron privacy is a core tenet of the ethics of librarianship. The American Library Association's *Privacy: An Interpretation of the Library Bill of Rights* (2019) emphasizes that protecting the privacy of library users is key to ensuring intellectual freedom because surveillance and monitoring produce a "chilling effect on users' selection, access to, and use of library resources." In 2005, librarians in Connecticut made headlines by standing up against the FBI and the USA Patriot Act to protect patron records (Cowan, 2006). Faced with a clear threat to privacy, these librarians sued the U.S. government in defense of their patrons' rights. However, the daily erosion of privacy facing patrons today is often more insidious and the day-to-day work of protecting privacy in libraries is less visible.

This issue of the *Oregon Library Association Quarterly* is dedicated to stories of how library workers across Oregon try—and sometimes struggle—to live up to our professional responsibility to protect privacy. These stories come from all corners of our library ecosystem, from public and academic institutions and from large and small communities. The articles presented here provide snapshots of some of the current challenges that libraries face around privacy, as well as some practical tips for dealing with these challenges. We have also included a short guide to relevant state laws, which we hope provides context for the issue as a whole. Although these authors describe varied topics, some key themes emerge from this collection of articles:

Privacy risks are not evenly distributed. Members of marginalized groups face additional surveillance and greater potential negative consequences. Many of the articles in this collection illustrate this point. As Kenna Warsinske describes, undocumented immigrants may be at risk of many types of seemingly harmless data being accessed by law enforcement to investigate their immigration status. Buzzy Nielsen and Jane Scheppke share their experience of enacting a new policy, intended to support safety, that resulted in the further marginalization of unhoused library patrons. Claudine Taillac notes that queer and trans teenagers exploring their identities may face censure at home or in the library for their reading and suggests some strategies for reducing that risk.

Protecting privacy isn't easy . . . Privacy threats are often baked into the very resources libraries provide. How do librarians balance the desire to provide digital content and use data analytics with privacy concerns? Jill Emery paints a picture of Oregon librarians' on-the-ground experiences with

Guide to State Laws

Oregon Revised Statute (ORS) provides for the protection of library patron records. Under ORS § 192.355, protection of "exemption from disclosure" includes "(23)(b) the name of a library patron together with the address or telephone number: and (23)(c) the electronic mail address of a patron" (Records; Public Reports and Meetings, 2021). The law also protects "(23)(a) circulation records, showing use of specific library material by a named person," (Records; Public Reports and Meetings, 2021).

For quick reference, the State Library of Oregon maintains an excellent LibGuide titled Library Laws of Oregon as a "selective compilation of the laws, rules, and legal issues directly affecting libraries in the state" (SLO, 2021). The American Library Association provides quick links to U.S. laws for 48 out of the 50 states (ALA, 2021).

References

American Library Association. (2018). State Privacy Laws Regarding Library Records. https://www.ala.org/advocacy/privacy/statelaws

Records; Public Reports and Meetings, ORS § 192.355; 192.502 (2021). https://www.oregonlegislature.gov/bills_laws/ors/ors192.html

State Library of Oregon. (2021). Library Laws of Oregon. https://libguides.osl.state.or.us/c.php?g=827876&p=5911054

licensing electronic resources and the challenges of negotiating with vendors around privacy, while Meredith Farkas argues that librarians should prioritize privacy more in the face of increasing data collection by library vendors and online services. Miranda Doyle provides insights into this complex privacy landscape in a school setting in the wake of the COVID-19 pandemic.

. . . but it can start with library staff. While it can feel daunting to get started, libraries can begin with such basic practices as reevaluating policies and updating staff training. As Buzzy Nielsen and Jane Scheppke discuss, the development and implementation of policies can offer opportunities to deepen a library's commitment to privacy and security for all users. Claudine Taillac outlines common public services interactions to consider for staff training, where customer service-oriented library workers may unintentionally infringe on user privacy.

Our privacy work doesn't end at the library doors. Sam Buechler and Tina Weyland both describe opportunities for librarians to advocate for privacy within their institutions, even when choices about invasive technology may be outside their immediate control. Given our professional commitment to privacy, library workers can ask important questions about practices and technologies in our broader communities, and collaborate to find other solutions.

These issues cross boundaries of library type and department. All library workers have a role to play in advocating for and safeguarding privacy inside the library, online, and within our parent institutions. As the pieces in this issue attest, implementing privacy requires staff training, a willingness to reevaluate current practices in light of new concerns, and sometimes looking outside the library to advocate for our users. We hope this issue sheds some light on how libraries in Oregon are already working on privacy protection, and highlights opportunities where we can continue to work together.

References

American Library Association. (2019, June 24). *Privacy: An interpretation of the Library Bill of Rights.* https://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy

Cowan, A. L. (2006, May 30). Four librarians finally break silence in records case. *New York Times.* https://www.nytimes.com/2006/05/31/nyregion/31library.html

Privacy in Practice:
Library Public Services and the Intersection of Personal Ideals

by Claudine Taillac
(she/her)
Assistant Director of Public Services, Jackson County Library Services
ctaillac@jcls.org

Claudine Taillac (she/her) is the Assistant Director of Public Services at Jackson County Library Services. In addition to Oregon, she has worked in public libraries in Arizona and California, with focuses on outreach, early literacy, circulation, and adult services, as well as special collections and archives projects. Outside of work, she spends as much time as possible enjoying nature with her partner, skiing, hiking, backpacking, biking, kayaking, and paddleboarding.

Anonymity. Confidentiality. Privacy.

These similar, yet distinct, concepts require nuance in a setting that is both public and highly personal. Your public library is just that: yours but also public. How do these concepts and the way individuals value them personally become reconciled within the library, a public institution that both safeguards and shares information? How do the privacy rights of adults and children, guardians and intimate partners, intersect and diverge at the library?

Privacy

This is one of our human rights. It is the right to exist without being observed or without anyone having information about your activities. Libraries, in accordance with the Code of Ethics of the American Library Association (1995), "protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired, or transmitted." In accordance with this, the Jackson County Library Services (JCLS) Patron Privacy and Confidentiality policy (2018) states, "We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired, or transmitted."

Librarians have a professional commitment to protect the privacy of patrons, as this is the cornerstone of the trust relationship between them and the public. This commitment must be resolute for freedom of information to be upheld. Libraries have a responsibility to create a collective definition, in the way of policy, of what patron privacy means. Contextualizing patron privacy necessitates creating a framework for the practicalities of implementation by frontline staff. Such a framework should consider anonymity, confidentiality, and privacy as they relate to the unique setting of libraries. For example, one way libraries are unique from an elementary school is that privacy is extended equally regardless of minor

age status. So while a teacher would have the ability to discuss all aspects of a child's school activity with a parent, this is not the case in the library setting. The uniqueness of this setting results in privacy practices that can surprise patrons and cause discord.

Clearly defining the reasons why patron privacy policy is written as it is gives staff the necessary knowledge and language to have privacy conversations with patrons. Staff having a deep understanding of the reasons behind patron privacy also creates more buy-in for policy compliance that benefits them during difficult patron conversations.

Anonymity

As public spaces, libraries cannot guarantee anonymity. Patrons who are able to gain access to the online catalog and digital resources, or who can call in for reference services, bypass the exposure of their library use by interacting with the library from the anonymity of their homes. In-person transactions for readers' advisory or reference services are a use-at-your-own-risk endeavor observable by others who are also using the space. However, anonymity in terms of someone being in the building is protected from third parties who may inquire about a patron's presence, such as family members or law enforcement.

Confidentiality

The two issues that come up around confidentiality are personally identifiable information (PII) and personal data (PD). Libraries retain PII in patrons' library accounts. These pieces of information are name, address, phone number, email address, birthdate, and driver license number. This information should not be shared or used inappropriately, and policy must include this assurance. PD covers more territory and can be understood as metadata—information that connects someone to their behavior, such as habits, likes, dislikes, friends, relatives, organizations—that combined will create a profile of that person. Whether inaccurate or accurate, this profile could be used to cause harm or violate privacy.

As the Assistant Director of Public Services for Jackson County Library Services (JCLS), it is my responsibility to ensure that frontline staff understand how and why patron privacy must be protected. An anchor for successfully fulfilling this responsibility is the Library Bill of Rights (American Library Association, 2019) statement VII: "All people, regardless of origin, age, background, or views, possess a right to privacy and confidentiality in their library use."

Much of the focus on library privacy currently centers on cybersecurity and internet privacy. These are crucially important issues for library IT departments and staff who oversee the ILS and e-resources. Following cybersecurity and internet privacy best practices can help ensure that patron privacy is being maintained. Librarians can design cybersecurity and internet security literacy programs, employing experts to help patrons understand risks and ways to protect themselves.

These, however, are not the privacy issues that frontline library staff encounter during patron transactions. The most common privacy scenarios frontline staff encounter are when dealing with holds release, youth accounts, readers' advisory, and people being sought by relatives or law enforcement. While patron privacy issues number more than these four, they are the foundation for the privacy training that frontline JCLS staff receive.

Holds Release

The JCLS holds release policy described in the JCLS Circulation Policy (2021) can be summed up by these principles:

- one user, one card;
- no linking accounts;
- no creation of PD.

Although protecting the privacy of patrons' accounts is not a new practice, a loose treatment of accounts can be common in libraries. Some couples or families are in the habit of sharing one card or using another family member's card because they've misplaced theirs. While staff cannot prevent these agreements between family members or the sharing of accounts, JCLS adheres to the "one user, one card" principle whenever possible. Not knowing whether a family member has given uncoerced access to their card to someone else, best practice is to encourage all family members to have their own accounts. Potential problems abound, such as one family member not returning materials on an account that is not theirs, resulting in fees for which the cardholder is responsible. Emphasizing the benefits of individual membership, such as being able to place more holds and check out more items—especially digital materials for which more limited checkouts are common—and helping children build a sense of responsibility in a low-risk way, are examples of how to soft-sell individual membership.

Recently, JCLS eliminated the practice of linking accounts for several reasons relating to privacy. Linking accounts creates PD by associating a person with someone else. Linked accounts can become problematic when someone's relationship status changes. Safeguarding patrons' accounts for the unforeseeable change in relationship status is a valid reason to not link accounts, even if a patron would prefer it. A linked account is never fully private, as both parties have access to each other's usage. At the least, in library systems where linked accounts are in practice, full explanation of the privacy implications of linked accounts should be shared with all patrons, no matter their age.

While having to provide the card or account number in order to pick up holds for someone else has been part of JCLS policy for a long time, compliance was low. In 2019, JCLS staff was given privacy training that emphasized compliance with this standard. Arguments for allowing others to pick up holds centered around ease for patrons and staff, and staff not wanting to have to enforce the policy, especially in the smaller libraries where a great deal of familiarity between staff and patrons exists. Knowing the status of someone's familial relationships should not intersect with library activity, even if this person is well-known to staff. This can lead to dangerous assumptions, as no one ever really knows what is going on in someone else's family. Poor boundaries often get confused with good customer service.

Setting clear and appropriate boundaries is one of the biggest challenges for many staff, especially if patrons have become accustomed to using someone else's account or picking up someone else's holds without having the card or account number. There are real and serious concerns surrounding noncompliance with this practice. Noted examples of this practice going awry exist, such as a husband picking up his own holds and asking if his wife had any holds he could also pick up. She did, in fact, and her holds contained books on divorce. Two consequences of this breach of privacy were staff fielding a call from the irate wife and a patron whose trust in the library had been broken. The consequences at home for the wife may have also been severe.

Youth Accounts

Youth accounts and parent or guardian access are areas where staff can use the most support from a clear privacy policy. Parents are accustomed to having unfettered jurisdiction over every aspect of their children's lives and believe that this will naturally extend to their children's library use. The ALA recognizes that children and youth have the same rights to privacy as adults. The JCLS Patron Privacy and Confidentiality policy adopted in 2018 states:

> The Library respects the privacy of all library patrons, regardless of age. Parents, guardians or caretakers of a child under age 18 who wish to obtain access to a child's library records, including the number or titles of materials checked out or overdue, must provide the child's library card or card number.

In February 2021, JCLS changed its Circulation Policy to create more privacy for youth cardholders yet allow for some parental/guardian access, although with clear rules. The changes included defining age tier permissions for parent/guardian access to a minor's card and the addition of a minor access card. The Circulation Policy states:

> The Library safeguards the privacy of all patrons no matter their age. A parent/guardian may have access to a child's record for which they are the responsible party according to the following schedule. In all cases, a parent/guardian requesting access to a child's record for which they are the responsible party must have the child's library card or card number. In all cases, Staff may not give access to the parent/guardian if the child has a Minor Access Card.

The schedule referred to is the age tier permissions. For youth 12 years of age and younger, if the parent/guardian who is the responsible party on the child's library card shows ID and has the minor's card or card number, staff may allow unrestricted access to the child's record. For youth ages 13 to 17, parents/guardians may pick up held items for the child if the parent has the child's card or card number. Parents may have information that allows them to settle fees. No other information may be disclosed. By keeping the granting permission in the hands of the child who must provide their card or disclose their account number for someone to have access, greater privacy is extended.

The addition of the minor access card serves two purposes. JCLS staff recognized that some youths do not have a stable home environment that allows for a parent or guardian to authorize them to get a full-service card. This unfortunate situation that is no fault of the children's limits their free access to information. The second reason is privacy. JCLS recognized that there are youth who feel they do not have support at home to read material they want or need. Following the ALA's standard that youth have the same rights to privacy as adults, this card with limited privileges (a two-item limit) and no financial penalty for loss or damage allows for unmonitored access. This is especially important for youth who are seeking information on sexuality or gender identity, substance abuse, depression, or who are in an abusive home situation.

Readers' Advisory

Providing patrons with readers' advisory (RA) services, while not immediately obvious as being a privacy concern, does have such implications. A lack of privacy in what one reads or views can significantly restrict library users' willingness to exercise their freedom to read, thereby impairing free access to ideas. When done correctly, RA includes recommending books without judgment while maintaining the privacy and confidentiality of the patron. During the interaction, key elements of protecting privacy are:

- being mindful to not ask the patron's name or to not use language that shows bias;
- asking questions to increase understanding but that avoid prying;
- speaking at a low volume level;
- avoiding commentary about reading choices—even if they are positive comments;
- using neutral language to create an environment where patrons feel their privacy is respected.

Privacy is a bias issue. Not having awareness of and thereby perpetuating bias can have a chilling effect on patrons. By eliminating prying questions and unsolicited opinions from the RA transaction, patrons will feel more comfortable seeking assistance even in relation to topics where discretion matters. Perceived judgment can feel like a violation of privacy. The consequence of this is that patrons may decide to not seek assistance when choosing books to read.

Third-Party Inquiries

While open observation is a possibility, and anonymity is not guaranteed when patrons are inside library buildings, divulging whether a patron is in the building must be safeguarded by staff as a privacy issue.

Consider this example: A visibly upset parent comes into the library and asks staff if their child has been at the library, explaining that the child has run away. The emotionality of the situation can cause staff to question the need to protect a patron's privacy. It is not uncommon for parents to ask staff to call them, or the police depending on the circumstances, if their child is seen in the library. While a child on their own has inherent dangers, there are sometimes dangers at home that may be the reason why a child has left. Staff cannot and should not make a judgment call either way.

It's difficult yet imperative to adhere to the privacy policy and explain to the parent the right of all patrons to undisclosed use of the space. Parents may look for the child on property, and the staff may go so far as to assure the parent that if they see the child, they will alert them that their parents are searching for them.

Similar situations occur with law enforcement, as officers are often unfamiliar with library privacy policies. Officers may freely search a library for an individual, but staff are not obligated to disclose whether they have seen the individual. A seemingly innocuous question by an officer, like the name of a person logged on to a public access computer, often makes staff question whether they can deny an authority figure they have been taught their entire lives to obey. Clear privacy policies and adherence to the ALA values on patron privacy help guide staff faced with these situations.

Equity, diversity, and inclusion (EDI) standards and policies are also an important aspect of protecting patron privacy. Libraries as refuges for the marginalized is a long-standing tradition. Immigrants who are living in the United States without the required documentation need assurance that their privacy and resident status will not become a barrier to seeking important resources they can access freely only at the library. The teenager looking for a safe place to access information on issues they don't feel safe discussing at home needs to know that their checkouts will not be shared with their parents. The person who has fled a domestic violence situation needs to know that their presence at the library will not be disclosed to their partner who is inquiring to staff about them.

Library workers, superheroes as they are, are humans first; sliding into lax habits regarding patron privacy will happen. Frontline staff have the added challenge, on top of their demanding jobs, to recognize when the library's privacy policy conflicts with their own ideals about parenthood, partnership, or the authority of law enforcement. One of the unique aspects of library work is how staff are required to set themselves and their opinions and beliefs aside when they are serving patrons.

Because some patrons can be at great risk when their privacy is not protected, adhering to policy must never be taken lightly. This is not to minimize the discomfort that doing so can produce in staff. Making a review of patron privacy an annual training will stimulate important conversations and ensure that the team's focus is on patrons first. It is a point of pride in library work to be looking out for patron privacy even when patrons do not know that you are.

References

American Library Association. (1995). *Code of ethics of the American Library Association.* https://tinyurl.com/2p8s5ar8

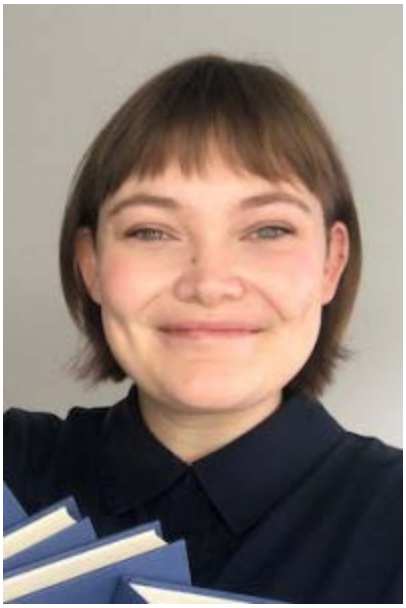
American Library Association. (2019). *Library bill of rights.* https://www.ala.org/advocacy/intfreedom/librarybill

Jackson County Library Services. (2018). *Patron privacy and confidentiality*. https://tinyurl.com/44rarbf9

Jackson County Library Services. (2021). *Circulation policy*. https://tinyurl.com/3zkc9nrb

Learning Better for the Next Thing:
Online Proctoring Services and Privacy Advocacy Outside the Library

by Sam Buechler
(they/them)
Student Success Faculty Resident Librarian, Washington State University Vancouver
sam.buechler@wsu.edu
@BuechlerSam



Sam Buechler (they/them) is the Student Success Faculty Resident Librarian at Washington State University Vancouver. Prior to their current position, Sam worked in circulation and access services departments at a variety of four-year and community college libraries. They have been a member of the Library Freedom Project since 2020. These experiences provide the foundation for their research which centers privacy and surveillance on college campuses and critical library pedagogy.

Introduction

In the fall of 2020, amidst the COVID-19 pandemic, higher education institutions found themselves with more time to consider how to best use and refine educational technology that had been urgently implemented or expanded during the spring and summer. Despite taking this additional time, it often felt as though the desire to provide normalcy—amongst abnormal conditions—took precedence over privacy protections. Examples such as promoting classroom engagement by requiring students to have their cameras on during synchronous online instruction illustrate this attempt to bridge normality within remote services. Another example of this tendency is online proctoring, in which the need to ensure academic integrity is used to justify the implementation of software that leverages surveillance and harmful technology.

I am employed at an institution that supports online proctoring as a method of instruction and has a contract with an online proctoring service, ProctorU. When I first learned this information, I felt a call to action. Just as a sense of urgency helped guide the implementation of online proctoring services, my own urgency guided my attempts at dismantling its use. Through this article, I will explain online and remote proctoring, the harms it poses to students, and why librarians should care about it. Furthermore, I'll outline my own efforts to eliminate proctoring software on my campus, how they fell short, and how we can envision better methods of dismantling surveillance.

Online Proctoring

Proctoring is not a new practice and has long been used to address concerns of academic integrity such as plagiarism and cheating; what is new is the increased use of online proctoring services. Online proctoring allows students to take tests that are monitored online through virtual proctors or algorithms. As a response to emergency changes in educational delivery,

online proctoring became more prominent—with certain proctoring companies claiming to have seen a 500 percent increase in use and subscription of their services (Caplan-Bricker, 2021)—and, unsurprisingly, so did the harms that they can cause.

Online proctoring generally implements an algorithm that determines when students are taking actions that can be considered cheating. Like many algorithmic technologies, online proctoring is filled with technological biases that directly impact folks with marginalized identities (Kelley, 2021; Swauger, 2020). Online proctoring and other forms of technological bias ultimately reinforce historical patterns of exacerbated surveillance, particularly of Black, Indigenous, and People of Color communities. This has long been researched and named by scholars such as Ruha Benjamin's (2019) "New Jim Code," Joy Buolamwini's (2016) "coded gaze," Safiya Umoja Noble's (2018) *Algorithms of Oppression,* and Virginia Eubanks' (2018) "digital poorhouse," among others.

This level of harm is seen in how online proctoring algorithms utilize facial recognition software that inaccurately captures darker skin tones or struggles to differentiate between individuals of different ethnicities. These algorithms also flag students for exhibiting specific actions related to disabilities (e.g. reading aloud, moving around) (Raji & Buolamwini, 2019;, Patil & Bromwich, 2020; Swauger, 2020). Furthermore, in order for the algorithms to even work, students must subject themselves to surveillance in order to begin the test, such as showing a form of identification that may not be indicative of their current gender identity, gender expression, or name (Swauger, 2020). Online proctoring also requires a significant amount of student labor that could better be spent studying. Before testing, students are often required to provide a 360-degree view of their space to ensure that the area is clean and free of people (Caplan-Bicker, 2021). This task is near impossible for students with childcare responsibilities, those living in multigenerational or multi-individual households, and those who are houseless. Finally, even without consideration to the exacerbated level of impact that online proctoring has on marginalized students, online proctoring impacts all students by adding additional stress factors during testing and invading their privacy (Caplan-Bicker, 2021; Harwell, 2020).

Library Workers as Privacy Advocates

Ultimately, there are many ways that online proctoring clearly affects students. At first glance, the issue of online proctoring still does not appear to be explicitly a library problem—it isn't distributed by the library nor is it readily available within the library or through our resources. Despite that, online proctoring affects privacy and intellectual freedom—core values of librarianship—and it is implemented within the broader systems we work in and contribute to. Within *Anonymity*, Alison Macrina and Talya Cooper write that "Librarians have long recognized the relationship between privacy and intellectual freedom; when we lack privacy, we can't have intellectual freedom, because we are less likely to read, write, and research freely when we fear that we're being watched" (2019, p. 2).

Proctoring technology exemplifies how being watched during the process of reading, writing, researching, and learning causes direct and lasting harm. Students do not have intellectual freedom when they have to mask their symptoms of attention-deficit/hyperactivity disorder (ADHD) symptoms so they don't get flagged for frequent movements, when they have to spend 20 minutes with lighting setup so cameras can pick up their facial expressions, or even when they feel they must resort to vomiting at their own desks in order to

not fail a test completely (Harwell, 2020). Macrina and Cooper provide the argument that library workers are "position[ed] to serve as advocates for political and regulatory solutions to threats to anonymity in our communities" (2019, p. 53). Library workers, particularly within academic libraries, do not work within a vacuum. As a result, when we choose not to act, when we interpret concerns that relate to our professional values as "outside" of our profession, we are also positioned as bystanders to harm.

A Study in Failure

Considering online proctoring and other surveillance technologies this way inspired me to act when my institution's provost sent out a campuswide email titled "ProctorU Statement," in late September (Chilton, 2020). By this time, there was already a vast amount of public knowledge available regarding the harms associated with online proctoring services including a recent data breach affecting ProctorU and its users (Patty, 2020). Given that students and families had begun asking questions about our continued use of the service, my expectation was for this email to mark its cancellation—it did not. Instead, this email attempted to answer or invalidate every possible concern that could be leveraged against the service and ultimately demonstrated a lack of understanding around some of the key harms that ProctorU perpetuates. For example, the email compared ProctorU security and data concerns to those of Instagram, Microsoft, or a bank's online platform without taking into account that the latter are voluntary services while the former is compulsory for student success in courses. Furthermore, the email also lacked any mention of the ways that ProctorU and other proctoring technology disproportionately targets and harms marginalized users.

This administrative email provided me with an immediate strategy in my quest to remove ProctorU from my institution: communicating how the concerns addressed within the "ProctorU Statement" were insufficient and still did not justify the continued use of online proctoring. As someone who was new to this institution, the first critical step in my path was to ask colleagues with institutional knowledge what kind of action was possible and likely to be met with success. That advice ultimately led to a lot of letter writing and meeting attendance. For example, I submitted a constituent concern to our faculty senate and brought my concerns to the attention of my campus's vice chancellor of academic affairs during a drop-in chat. After speaking and writing about this on my own, I eventually partnered with another library colleague and my campus's Accessibility Council. Through this partnership, we performed concrete outreach (e.g., presenting at Washington State University's Diversity Summit) and developed informational material for faculty who may use ProctorU in their classes (e.g., a white paper regarding the harms of ProctorU).

We were making additional headway by incorporating student leaders into these efforts and seeking feedback for our white paper when we encountered rapid changes regarding ProctorU occurring outside of our influence. First, ProctorU announced that it was moving away from an exclusively algorithmic model and then, as we moved back to in-person instruction, our campus stated that ProctorU would only be used for the Global Campus online courses. The latter ultimately became a natural stopping point in our continued action as many of the members of our team had found it to be a sufficient answer to our concerns—and in many ways it is. It is good progress that the majority of students at our institution no longer experience online proctoring, but it's not perfect. ProctorU is still on our campus, online students are still subjected to it, and, critically, there are currently no structures or agreements in place to keep it from expanding systemwide again.

A Vision of Doing Better

At this point, efforts towards removing ProctorU entirely from our campus have stagnated and it is through reflection that I have been able to see how efforts towards this and related goals can be reinvigorated. Primarily, I have been able to recognize that the largest gains in progress towards this goal occurred only when I began to work closely with others. This idea is most often elaborated amongst organizers who see a difference in individual and collective work. This is succinctly explained in an interview between Eve L. Ewing and Mariame Kaba included in Kaba's book, *We Do This 'Til We Free Us* (2021). Specifically, Ewing and Kaba (2019) explain the difference between activists and organizers. Kaba describes activists as

> folks who are taking action on particular issues that really move them in some specific way, but activism only demands that you personally take on the issue. That means signing petitions, being on a board of a particular organization that's doing good in the world. (p. 180)

This description of activism aligns with my beginning steps towards removing ProctorU and bringing information about surveillance in educational technology on my campus. I wrote to the faculty senate, I wrote blogs and tweeted thoughts, I researched continually and extensively to stay up to date on frequent changes and reporting. This was all individual action; even early communication with others served to seek advice on how to make change alone, where it could have instead been moments to build collective action.

The attempt to build a movement without community is where my effort stalled. Progress towards removing online proctoring at our institution began only when I started working closely with others. More people joining our efforts meant more ideas were brought to the table, more institutional knowledge was available, and we had a wider base to establish connections. This aligns well with Kaba's (2019) description of organizing:

> Organizing is both science and art. It is thinking through strategy, and then figuring out who your targets are. It requires being focused on power, and figuring out how to build power to push your issues, in order to get the target to actually move in the way that you want to. (p. 181)

By the time a shift was made to building a community of people acting towards a common goal, the use of ProctorU on our campus changed. Primarily, conditions changed in a way that left some of us feeling as though we had reached a satisfying conclusion. Our group hasn't been able to move beyond this initial progression because, amongst other external factors, we lacked the time needed to build a strong common goal as well as the resilience needed to continue working towards it.

When it comes to our stagnation in continued action, I think of adrienne maree brown's book *Emergent Strategy: Shaping Change, Changing Worlds.* A key facet of brown's vision of emergent strategy is "Moving at the speed of trust. Focus on critical connections more than critical mass—build the resilience by building the relationships" (brown, 2017, p. 42). When we fail to do this, we can end up with results similar to that of my own experience—where we come to a conclusion in action not because it meets an end goal, but because we haven't built the relationships needed to push past initial progress towards something that works for all of us.

As a profession, and as individuals, we can start to move at the speed of trust by building or joining communities centered on privacy advocacy and privacy-mindedness before the next wave of surveillance technology is implemented within our communities. There are spaces within our field writ large (e.g., the Library Freedom Project) but we also need to understand the unique situations in our places of work, in our institutions, and in our communities that can benefit from our expertise as library workers. Symphony Bruce (2020) provided an example of this in a Library Freedom Institute session where she spoke on building a community of practice among staff, faculty, and administrators at her institution. Bruce (2020) explained that her success came in finding an "inciting incident" that could engage folks, particularly those with broader scopes of responsibility and influence, with the work of privacy advocacy and then organizing them around their reactions to that incident through education and action.

For me, it was a colleague who felt as strongly as I do about our use of ProctorU and the Accessibility Council on my campus who saw it as an issue for students with disabilities. By utilizing emergent strategy and organizing principles, we can start building stronger connections with partners across the systems we work in and build stronger movements as a result.

Conclusion

The use of online proctoring technology is my example of an inciting incident, but it is not the only example of technological harm on our campuses and within our communities. Through my attempt to remove online proctoring from my institution, I have found a distinct difference between individual and collective action. Taking time to build a strong community with a shared vision is crucial to ensuring that we not only remove surveillance technology but also prevent its continued invasion. Comparable technological surveillance is being implemented around us daily (e.g., facial recognition software, video doorbells) and it's essential that we know how to leverage our knowledge as library workers to enact change and prevent harm; and critically, we have to remember that we must do it together.

References

Benjamin, R. (2019). *Race after technology: Abolitionist tools for the New Jim Code.* Polity Press.

brown, a. m. (2017). *Emergent strategy: Shaping change, changing worlds.* AK Press.

Bruce, S. (2020, October 15). *Building communities of practice: Privacy talks with staff, faculty, & administrators.* [Presentation at Library Freedom Institute]. Library Freedom Institute.

Buolamwini, J. (2016, November). *How I'm fighting bias in algorithms.* [Video]. TED. https://tinyurl.com/yhd4fe42

Caplan-Bricker, N. (2021, May 27). Is online test-monitoring here to stay? *The New Yorker.* https://tinyurl.com/2p9e9f69

Chilton, E. S., Cillay, D., & Pillay, S. (2020, September 25). *ProctorU Statement.* Washington State University. https://from.wsu.edu/provost/2020/ProctorU/166027-browser.html

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor.* St. Martin's Press.

Ewing, E. (2019, Fall) Mariame Kaba: Everything worthwhile is done with other people. *ADI Magazine.* https://tinyurl.com/2s3t3bjs

Harwell, D. (2020, April 1). Mass school closures in the wake of the coronavirus are driving a new wave of student surveillance. *The Washington Post.* https://tinyurl.com/2p9y4cmr

Kaba, M. (2021). *We do this 'til we free us: Abolitionist organizing and transforming justice.* (pp. 176–186). Haymarket Books.

Kelley, J. (2021, June 22). A long overdue reckoning for online proctoring companies may finally be here. *Electronic Frontier Foundation.* https://tinyurl.com/bdcr6efa

Library Freedom Project. (n.d.). *Library Freedom Project*. https://libraryfreedom.org/

Macrina, A., & Cooper, T. (2019). *Anonymity*. American Library Association.

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. New York University Press.

Patty, A. (2020, August 6). Hackers hit university online exam tool. *The Sydney Morning Herald.* https://tinyurl.com/ycks3ucy

Patil, A. & Bromwich, J. E. (2020, September 29). How it feels when software watches you take tests. *The New York Times.* https://tinyurl.com/2p886t9e

Raji, I & Buolamwini, J. (2019). *Actionable auditing: Investigating the impact of publicly naming biased performance results of commercial AI products.* Conference on Artificial Intelligence, Ethics, and Society. https://tinyurl.com/szhp3n8w

Swauger, S. (2020, April 2). Our bodies encoded: Algorithmic test proctoring in higher education. *Hybrid Pedagogy.* https://tinyurl.com/dx2zx94u

Don't Deputize Intolerance:
Keeping Your Security Policies Safe from Your Patrons

by Buzzy Nielsen
(he/him)
Program Manager for Library Support & Development Services, State Library of Oregon
buzzy.nielsen@slo.oregon.gov

and by

Jane F. Scheppke
(she/they)
Former Assistant Director of Library Services, Crook County Library
piggy4yourmoney@gmail.com

Buzzy Nielsen (he/him) is the former Director of Library Services at Crook County Library in Prineville, Oregon. He has spent most of his career in small and rural libraries throughout Oregon. You probably receive more email from him than your best friend due to his current role as Program Manager for Library Support & Development Services at the State Library of Oregon.

Jane F. Scheppke (she/they) is the former Assistant Director of Library Services at Crook County Library. As of December 2021, they are a digital multimedia artist based in Salem, but the future is wide open. By the time this goes to print, they could be a master machinist and father of four based in Schenectady. Reality is what you make it.

To live in rural Oregon is to live in tension. Crook County exemplifies the tensions of living in rural Oregon in many ways, and not just because it is located dead center in the middle of the state. It also encapsulates the contradiction of some residents trying to keep a hold on a past they perceive as idyllic, while others live with the opportunities and harsh realities of the present. Crook County sees this contradiction reflected in its reliance on industries both historic and modern: ranching, wood products, and auto tires on the one hand, and data centers, health care, and hemp on the other. This tension can boil over into conflict, even when it comes to something as supposedly simple as a change in library policy.

Like in many other communities suffering identity crises, some people in Crook County, and its only incorporated town of Prineville, ran afoul of the rising use of opioids (Chaney, 2019). Those of us at the public library saw the effects firsthand. In 2018 and 2019, the library faced a confluence of opioid-adjacent situations:

- finding needles, intravenous drug paraphernalia, and vomit on library grounds;
- patrons in the building who were apparently unconscious, not just sleeping;
- someone going through severe opiate withdrawal while visiting a social worker; and
- the departure of the county mental health provider, Lutheran Community Services Northwest, which had been operating a day center that drew in unhoused people. (McCallister, 2021).

These incidents presented a serious security dilemma for the library where we worked as director and assistant director: How do we ensure safety for the most vulnerable patrons, including those experiencing adverse effects from drugs, while generally keeping the library welcoming for everyone? This dilemma led us to two security-related decisions: to forbid sleeping in the library and to install security cameras. Both decisions ultimately demonstrated how choices made, ostensibly, to protect patrons' physical safety, or to help some people feel more "secure," can adversely impact safety for patrons who are already marginalized.

No Sleeping in the Library; No Rest for the Downtrodden

As in many rural communities, some Crook County residents think certain other people don't "fit in" to the community or its idealized cowboy past. It is not uncommon to hear conversations or see online comment threads, even involving police and city/county officials, that "those people" are ruining Prineville. Many of "those people" gravitate to the library: individuals without permanent housing, LGBTQ+ teens, people of color, unemployed individuals, and so on. The Crook County Library is a place where these besieged individuals can get things unavailable to them elsewhere: computers and Wi-Fi, restrooms, shelter from extreme weather, space where they won't be bothered, or even simply a staff member that says hello and acknowledges them.

Sometimes, these and other people slept in the library. Some had nowhere else to go (neither of Prineville's two shelters were open during the day), some had stressful lives even if they had a house to stay in at night, and others just drifted off while reading. The building's quiet alcoves and cozy, living room-like seating areas encouraged dozing. Nevertheless, other patrons were quick to point out this behavior to library staff, particularly when people laid down on sofas. The appearance of opioid paraphernalia—which at this point was just beginning to occur—raised concerns that some people, thought to be dozing, were actually overdosing or "nodding off." As a result, frontline staff often requested rules prohibiting sleeping.

At the 2018 Oregon Library Association Conference, Jane, who was Crook County Library's assistant director at the time, was surprised when most attendees at a panel on weapons in the library confirmed that their libraries had policies forbidding sleeping. Several participants pointed out that it is difficult to tell whether a patron is truly asleep, or unconscious due to a medical emergency. This resonated with Jane, as staff at Crook County had recently called 911 after a man found sleeping could not be roused. There had also been an incident where a woman in the computer lab had gone into diabetic shock. While this patron had recognized her symptoms and was able to alert staff, conference attendees pointed out that other patrons in similar situations might appear to simply fall asleep. Other participants noted that patrons with post-traumatic stress disorder (PTSD) often had outsized startle responses that could escalate to violence, making it dangerous for staff or other patrons to wake them.

Upon her return to Prineville, Jane requested that the library's Code of Conduct be revised to forbid sleeping on library grounds. On May 10, 2018, this change was proposed and adopted by the Library Board of Trustees, adding the language "do not sleep, appear to sleep, or camp" (Crook County Library, 2018). The new policy was justified primarily to preserve the safety and health of the sleeping patrons themselves. Jane also noted that by snoring or taking up undue space, sleeping patrons could disrupt others.

The change was enacted with an unusual provision—the policy would go into effect on July 1, not immediately upon adoption by the Board. Staff felt that patrons should be given adequate notification of the new policy, so they would not be penalized unfairly for violations. Immediately after the change was adopted, signs went up around the library advertising the policy change and explaining its pro-safety intent. These signs were favorably remarked upon by patrons, particularly those who were unlikely to be sleepers themselves; "about time" was a common refrain from the public.

Meanwhile, management trained staff not only in how to wake patrons without touching them, but the trainers also tried to communicate that sleeping was not a harmful activity in and of itself. Sleepers were to be treated with empathy and kindness. It was specified that staff could not trespass a patron for sleeping without the intervention of a manager or designated Person in Charge. This differed from past training on Code of Conduct enforcement, which tended to emphasize progressive discipline. It also deviated from the library's separate Use Restrictions Policy, which gave leeway for staff discretion to enforce policies but did not distinguish between "red" rules that always must be followed to the letter (e.g., no alcohol consumption) and "blue" rules that could be bent in some circumstances to help create equity, for example, maintain a reasonable speaking volume (Dowd, 2018, pp. 213-214). These deviations from standard practice confused some staff, especially those who had been punished by previous management for not following "the letter of the law." As a result, staff needed frequent reminders about proper enforcement.

Unfortunately, signs advertising an imminent policy change proved to be too enticing in a community where a small but noisy contingent pined for vigilante "cowboy justice." Enlisting themselves as self-styled "Nap Mastersons," a handful of patrons took it upon themselves to patrol the library for violators. If we were lucky, patrons informed the staff of sleepers, who then took appropriate action. On a handful of occasions, though, patrons woke the sleepers themselves. In taking the policy into their own hands, patrons risked their own safety while often violating the dignity and safety of the sleeper.

The potential for privacy violations among the vigilantes was high. Patrons often drifted off among stacks of library materials. When "vigilante" patrons attempted to wake a sleeper, they often committed the cardinal no-no of touching the sleeper—a massive violation of personal space (and remember those outsized startle responses?)—and in doing so got close enough to snoop the sleeper's book selections. Given that the rule enforcers often justified their actions based on whether or not the sleeper had a "valid reason" for being in the building ("all they're doing is sleeping and reading comic books!"), the reading, viewing, and listening material of sleeping patrons likely came under scrutiny during these interactions.

This sudden influx of patron enforcers, combined with the challenge of encouraging a previously micromanaged staff to enforce policies with empathy, led to even more trepidation for the library's next decision on safety and security.

Who Secures the Security Cameras?

The circumstances that led to the adoption of our no-sleeping policy did not abate, and by the end of 2018 we began to consider security cameras as another necessary measure. First, the evidence of drug use on the library grounds posed an immediate physical safety hazard. Paraphernalia was found on the patio of the very popular library meeting room, which often hosted parties and other events frequented by children. The potential of a child picking up and playing with a needle was real.

Second, the appearance of needles in the courtyard coincided with a marked increase in the number of mandatory reporter calls made by library staff. Public library staff in Oregon are statutorily required to report suspected incidents of child abuse and neglect (Oregon Department of Human Services, 2021). Sexual harassment of patrons and the nearly all-female staff also seemed to be picking up in frequency, as indicated anecdotally and in internal incident logs.

Third, through behind-the-scenes conversations, the library was being pressured by local law enforcement and county officials to limit the 24/7 Wi-Fi. Officials claimed, without evidence, that the availability of free internet during off-hours was causing unspecified "problems." We were loath to limit hours, given that the library was one of the few sources of public Wi-Fi that did not require a purchase or interaction with a customer service employee. Some of the same individuals alleged to be causing problems after hours also used the library during the day because they had nowhere else to go.

The library's troubling experience with the no-sleeping policy heightened our concerns about adding cameras. The increased surveillance could easily become a tool to police and invade the privacy of the library's most vulnerable individuals, including many of the same patrons targeted by the self-appointed sleep sheriffs. This potential for surveillance abuse was not theoretical. Members of the local neighborhood watch—a group very invested in the idea of Prineville as a "good" community—were interested that the library was considering installing security cameras. Both watch members and law enforcement felt that cameras could be used to investigate neighborhood happenings.

We ultimately decided to install the cameras in April 2019. They were a compromise that allowed us to retain 24/7 Wi-Fi, while hopefully discouraging drug use on library grounds. But our experience with the no-sleeping policy led us to limit who could access the footage and when, including:

- Retaining the footage for only one week.
- Locating cameras only on the exterior of the building and interior parts with limited visibility. No cameras were put in areas where protected patron activity might be exposed: the front desk, children's room, computer lab, meeting rooms, and common seating areas.
- Narrowing views of exterior cameras to only cover library grounds, not to the wider neighborhood.
- Requiring a formal public records request for non-library staff to review footage.
- Purchasing a system that was self-contained and not connected to any other Crook County system, to limit law enforcement's ability to review footage without permission or cause.

Although it's unclear whether these provisions were responsible, the cameras created fewer problems than the no-sleeping policy. Their presence appeared to reduce the drug paraphernalia found on library grounds. The footage also was not requested by the public or by law enforcement, perhaps because we chose not to widely publicize the cameras and only posted inconspicuous signs at the entrances. And fortunately, we found little need for the footage aside from one time when we unsuccessfully tried to find out who started a literal dumpster fire on the Fourth of July and another time when there was a mistaken case of bike theft. But the mere existence of the camera footage meant that abuse was a real possibility.

Lessons Learned

From the point of view of the local neighborhood watch, the library was doing a bang-up job protecting the community Old West-style with its sleeping ban and security cameras. We were not so sure. In enacting these changes, we realized that the actions we'd taken to protect the immediate physical safety of all our patrons were being used to violate the safety and security of specific patrons. It just so happened that all of the patrons being identified as violators were unhoused, or were teenagers, or were Black, Indigenous, or People of Color (BIPOC), while the enforcers overwhelmingly belonged to more privileged demographics. What could we have done to avoid creating these inequities?

When libraries create policies or enact tools to change patron behavior, we recommend that they start with these three basic premises:

1. Everyone belongs at the library.
2. All library patrons, regardless of personal factors including age, ability, and housing status, are rational actors with dignity.
3. Not everyone agrees with premises 1 and 2, and may never agree despite your best efforts.

When we wrote the no-sleeping policy and installed security cameras, our first priority was protecting the physical safety of our patrons and staff. Given the frequency of sleeping patrons and needle discoveries, it seemed like an opioid-related disaster—an overdose, a child stuck with a needle—was imminent, and that we needed to move quickly. In our haste to get policies drafted and enacted, however, we neglected to consider issues of safety and security beyond our own privileged point of view. We didn't consider how these policies would be interpreted by the people they were intended to protect, or how some might use the policies to justify harassing marginalized groups whom they perceived as "not belonging."

In hindsight, we still believe that the security cameras were needed to protect the immediate safety of staff and patrons. We also believe that we made the right call when we instructed staff to wake sleeping patrons, as we had several incidents both before and after the policy change in which "sleepers" turned out to be having medical crises. However, we could have made choices to mitigate the negative consequences of our policy changes. If we had to do it over again, we'd give our past selves the following advice.

Slow Down

Neither of us have seen a dead body on the job yet, and we were in a hurry to ensure we never did. In situations where an immediate safety risk has made itself known, there are certain actions you can take immediately (like installing sharps containers in accessible places)

and some actions that require more consideration. Changing a policy, or taking an action that could violate the privacy of library users, are both examples of the latter. Not every complaint made by staff or patrons rises to the level of action, and very few rise to the level of immediate action.

Identify Staff Training Needs, and Change All Relevant Policies

Crook County Library had separate Code of Conduct and Use Restrictions policies. The former outlined what you couldn't do at the library, while the latter outlined the possible consequences for misbehavior. While the Use Restrictions Policy was written to give staff leeway to enforce rules, it essentially treated all Code of Conduct violations as equal; the policy did not explicitly permit staff to bend a rule to preserve equity, or to assist a disadvantaged person. If your staff have been punished for not following policies exactly as written in the past, the idea that some rules might need to be bent will not be readily accepted, to put it mildly.

Ask Yourself: Are You the Best Trainer for the Job?

While the *Librarian's Guide to Homelessness Academy* (Dowd, 2018), available free through the State Library of Oregon, is not without flaws, library staff at Crook County seemed more receptive to concepts of compassionate enforcement when they were presented by the author, Ryan Dowd. In rural Oregon, "authority" often looks more like a guy like Dowd (masculine, physically large, confident) than like Buzzy and Jane (who are basically what happens if NPR tote bags could walk, talk, and get master's degrees).

Avoid Blanket Bans on Behaviors that Don't Hurt Anyone

Don't punish people for doing what they need to do to stay alive. Sleeping, eating, drinking, and yes, even bathing do not cause problems in and of themselves. Rules banning these behaviors, rather than their harmful causes or effects (such as doing drugs or making messes), are ripe for abuse by the privileged against the underprivileged. They're also guaranteed to be inconsistently enforced. (Consider, would you prohibit a baby from doing any of these activities? How about a senior adult?)

Instead of a Policy, Write a Statement

What kind of grief might we have avoided if, instead of banning sleeping for all library users, we trained staff how to safely wake people while simultaneously asserting patrons' right to sleep? It might go something like this: "Sleeping is an activity that harms no one, essential for the health and well-being of all people. Recently, people having medical emergencies have appeared to fall asleep and have been unable to wake up. For this reason, library staff may choose to wake you up if you fall asleep. However, there is no rule prohibiting sleeping at Crook County Library. If you suspect someone is having a medical emergency, call 911 and alert library staff immediately." Such a statement outlines both patron and staff rights and responsibilities while explicitly affirming that library staff, and not patrons, enforce rules.

Make It an Offense for Library Users to Enforce Policies on Their Own

If your behavioral policy defines harassment, make the malicious enforcement of library rules by non-library staff a part of that.

Policies that make some people feel secure—especially people who may not perceive the past or present levels of inequity in their community—don't necessarily make all of your patrons safer. Instead, those policies can become weapons that some in your community wield against those they feel don't belong, just like when a Wild West posse rode strangers out of town on a rail. Libraries alone cannot solve the underlying tensions that cause conflict within their communities. But they can be cognizant and careful of how those tensions can play out when changes are made in the name of safety, just as we learned in Crook County, where the Old West meets Big Data.

References

Chaney, J. (2019, March 12). Tackling the Crook County opioid crisis. *Central Oregonian.* *https://tinyurl.com/2p9ehumy*

Crook County Library. (2018, May 10). *Board of Trustees meeting.* https://tinyurl.com/2p8ej83r

Dowd, R. (2018). *The librarian's guide to homelessness: An empathy-driven approach to solving problems, preventing conflict, and serving everyone.* ALA Editions. https://www.oregon.gov/library/libraries/Pages/tutorial-registration.aspx

McCallister, R. (2021, January 19). Expanding and providing an inclusive space. *Central Oregonian.* https://tinyurl.com/2ttjwpr5

Oregon Department of Human Services. (2021, November 11). *Mandatory reporting of child abuse.* https://www.oregon.gov/dhs/abuse/pages/mandatory_report.aspx

Safeguarding Student Privacy in Schools

by Miranda Doyle
(she/her)
District Librarian,
Lake Oswego School District
doylem@loswego.k12.or.us
@MsMintheLibrary

Miranda Doyle (she/her) is a District Librarian at Lake Oswego School District. Before she switched to school libraries, Miranda was a Young Adult Librarian and then a Branch Manager for the San Francisco Public Library. She is currently serving as a member of the Oregon Intellectual Freedom Committee. In her spare time, Miranda enjoys running, kayaking, and learning Brazilian jiu jitsu.

Schools have always collected data on their students—everything from grades and test scores to information about behavior and medical issues. Beginning in March 2020, however, the potential for unwanted sharing of student information exploded. Most schools without existing 1-to-1 technology programs, where every student is assigned a digital device, scrambled to hand out laptops, Chromebooks, or iPads to students. Schools also tried out and adopted digital teaching tools such as Google Classroom, Canvas, Clever, Pear Deck, Flipgrid, Edpuzzle, Screencastify, Explain Everything, Kahoot!, GoNoodle, and many others. The COVID-19 pandemic pushed many schools fully online. Now, with schools back to in-person learning, school activities still often depend on the use of these digital devices and tools.

Parents and guardians of preschoolers have some power to limit how much data children share. However, after these children enter kindergarten, they are usually required to use online learning platforms to access and turn in assignments. Even if schools allow parents and guardians to opt their children out of taking a device home or using specific apps, opting out can make it very difficult for students to participate in classes. For example, if students use Chromebooks and teachers use Google Classroom to post assignments, an opted-out student would not be able to take part in learning activities or even know what homework they're responsible for. A study conducted in the summer of 2021 concluded that more than one in three parents said they were "very concerned" about security and privacy issues around their student's data (Klein, 2021b).

School administrators must consider the digital rights of these students and families as they choose resources. It's also important for parents, teachers, school librarians, and the broader community to know the types of data that schools and their third-party vendors collect, and what they can do to better protect that data.

Multiplying Devices and Apps

Before the pandemic, only some schools provided a device for each student to take home. Now most do. A February 2021 survey by the EdWeek Research Center found that 42 percent of schools gave each elementary student a digital device before the pandemic, but that number doubled to 84 percent by the middle of the 2020–21 school year (Klein, 2021a). The same survey found that 90 percent of middle and high schools issued 1-to-1 devices. As schools increasingly use cloud-based services such as Google Classroom and Google Drive, they are turning over huge amounts of information to technology companies.

In addition, many school districts now use threat detection and prevention software to monitor online activity (Herold, 2019). Private companies offer schools 24/7 monitoring and alerts, searching student emails, files, and social media for keywords and images.

Why worry about data collection and privacy? For one, this collected information can be used in ways that are inequitable and damaging. In one horrifying example, a school district in Florida shared student data with the police department, including grades, disciplinary histories, and whether the students had experienced trauma (Lieberman, 2021). The police department then used the data to compile "a secret list of middle and high school students it deems as potential future criminals."

In addition, data leaks and ransomware attacks on schools are common. One investigation found children's personal information, directly from school files, for sale on multiple websites (Collier, 2021). School districts, along with hospitals and other large organizations, have become a target for hackers. Some school districts have paid hackers to restore access to their student information systems, or refused to pay. Locally, Portland's Centennial School District experienced a data breach and discovered that district data was posted online | (Ramakrishnan, 2021).

Third-Party Vendors and Student Privacy

Schools often contract with multiple third-party vendors for cloud-based software and services to track student attendance, test scores, educational plans, student work samples, health information, and other data. Teachers also sign their classes up for educational apps and websites—classroom social media sites, typing or math practice, ebook providers, and much more. Districts should develop and adopt privacy policies, and should evaluate new and existing online services to make sure they don't share student data or collect more information than is necessary.

However, even school districts with a thorough process for investigating privacy policies must depend heavily on vendor claims. Districts aren't often able to scrutinize the company's actual practices. For example, many school districts now issue Chromebooks to students and enroll them in Google Apps for Education, which includes Google Docs, Classroom, and Drive. While these tools are useful (and the basic version is free to schools), some have questioned how Google uses children's data. Google says it does not collect information on students for advertising purposes, but that may not always be true. In 2015, the Electronic Frontier Foundation filed a complaint with the Federal Trade Commission alleging that Google was tracking students and building profiles on them. Google claims to have changed its practices in response (Cope, 2016).

In September 2019, Google paid a $170 million fine for violating the federal Children's Online Privacy Protection Act (COPPA) after regulators said that Google-owned YouTube

"knowingly and illegally harvested personal information from children and used it to profit by targeting them with ads" (Singer & Conger, 2021). So, even companies that have strong written privacy policies might not always follow their own rules.

Video Platforms in Schools

In March 2020, many schools started conducting classes over video platforms such as Zoom or Google Meet. This raised new privacy concerns. Because there was little advanced planning, most schools—and school librarians, who often assisted with the transition—jumped to video platforms without time to vet policies, procedures, and tools. Public libraries also dealt with these issues as they implemented online library programming such as author visits, trivia nights, and guest speakers. Now, even with in-person events returning, video meetings are still used—for parent conferences, for example.

Many questions surround schools' use of video conferencing platforms. For example, what data do Zoom and other platforms collect about students? How secure are these platforms? Where are the videos stored? How long will schools keep them? Screen captures made by students or other participants in a meeting can also violate privacy, as when a student records and shares a clip. Teacher trainings have also been recorded by an attendee—this issue surfaced in Oregon when clips from a Beaverton School District Zoom meeting appeared in the news and on social media and created an uproar (Marnin, 2021). Additionally, teachers and other school staff are faced with the issue of seeing or hearing problematic things while on a Zoom call. While teachers are mandated to report abuse or neglect, there is also the potential for over-policing, as when police went to a Black seventh-grader's house because he was playing with a Nerf gun during an online art class (Peiser, 2020).

Privacy in the School Library

School libraries also need to be concerned about their own data collection. For example, school librarians can ensure that library circulation records aren't stored in their circulation system forever, and that notes left on patron records are deleted regularly. School libraries should make sure that their ebook and database providers follow laws about collecting personal information about students and their reading or research habits. When the Statewide Database Licensing Advisory Committee chooses databases for libraries in Oregon, for example, privacy is an important criterion in the selection process.

Print books and materials aren't exempt from privacy issues. For example, should school libraries send overdue notices directly to parents? Does this inhibit students who might otherwise borrow books on sensitive topics? School libraries may also keep a student's checkout records in their circulation software and ebook platform even after items are returned. What if a parent, teacher, principal, or law enforcement officer comes into the library to ask which books a student has borrowed? School libraries often deal with such privacy concerns differently from public libraries.

Schools, parents, guardians, and concerned community members can help address these issues using a variety of strategies. They can learn more about the federal and state laws regarding data collected about children. The Children's Online Privacy Protection Act (COPPA) and the Family Educational Rights and Privacy Act (FERPA) guide the manner in which service providers and schools can use or release student information. Schools can write or strengthen privacy policies with input from all the stakeholders. Schools can choose third-party vendors who do not sell student information or track students for advertising

purposes. This might mean paying for digital services, so that companies earn revenue from subscriptions rather than from collecting and selling student data. Sometimes schools and libraries can choose which records to collect, and decide not to store personally identifying information beyond the minimum required. Families and community members can ask which services and tools students use in class.

All of these steps are important in making sure student data is as secure as possible, and that it is used only to advance educational goals.

References

Collier, K. (2021, September 10). Hackers are leaking children's data—and there's little parents can do. *NBC News*. https://tinyurl.com/2t2ujvns

Cope, J. G. (2016, October 6). Google changes its tune when it comes to tracking students. *Electronic Frontier Foundation.* https://tinyurl.com/2p87p4s6

Herold, B. (2019, May 30). Schools are deploying massive digital surveillance systems. The results are alarming. *Education Week.* https://tinyurl.com/yr5j9vwb

Klein, A. (2021a, April 20). During COVID-19, schools have made a mad dash to 1-to-1 computing. What happens next? *Education Week.* https://tinyurl.com/2p8nx3nh

Klein, A. (2021b, November 16). Ed tech usage is up. So are parent privacy concerns. *Education Week.* https://tinyurl.com/bdfk2edx

Lieberman, M. (2021, February 23). Using student data to identify future criminals: A privacy debacle. *Education Week.* https://tinyurl.com/nsbtjb9z

Marnin, J. (2021, May 28). Twitter outraged over teacher telling educators to embrace anti-racist thinking or be fired. *Newsweek*. https://tinyurl.com/4ead4huw

Peiser, J. (2020, September 8). A Black seventh-grader played with a toy gun during a virtual class. His school called the police. *Washington Post.* https://tinyurl.com/yc3rc233

Ramakrishnan, J. (2021, April 26). Centennial schools to close for 2 days after hackers breach school technology systems. *The Oregonian*. https://tinyurl.com/3tv83drp

Singer, N., & Conger, K. (2021, August 10). Google is fined $170 million for violating children's privacy on YouTube. *The New York Times.* https://tinyurl.com/2p9dma9p

Beyond HTTPS and the Cloud:
Building a Safe and Secure Web Resource for DACA and Undocumented Students

by Kenna Warsinske
(she/her)
Analyst Programmer 2,
Valley Library,
Oregon State University
warsinsk@oregonstate.edu

Kenna Warsinske (she/her) is an Analyst Programmer 2 (website developer) for the Valley Library at Oregon State University. She also volunteers to provide digital privacy and technical support for activists and local politicians. Kenna built her very first website in the small computer lab at her middle school library.

In 2016 and 2017, after the election of Donald Trump, the Deferred Action for Childhood Arrivals (DACA) program was in danger of being suspended or revoked entirely. This left many Oregon State University students in legal limbo, impacting their success as students as well as their ability to pay for college. The Department of Homeland Security, especially the small department Immigration and Customs Enforcement (ICE), ballooned in influence with the new administration. Trump had made anti-immigration a cornerstone of his campaign and that did not slow down once he took office. Undocumented students were now staring down new legal and financial challenges that were well outside their (and university) control. The university needed to respond quickly to changes in immigration policy, aid students who were struggling, and have one central location for advisors and students to find resources.

The Oregon State University (OSU) library got involved in the university's effort to help DACA and undocumented students. At the time, relevant resources were siloed across campus, so it was difficult for students to know what resources were available. Even advisors couldn't navigate the various systems. For example, on the OSU website, the Admissions page and Student Legal Services page both had relevant information, but they didn't refer back to one another. To help resolve this problem, the library offered to gather the resources distributed across campus for undocumented and DACA students.

After the resources were collected, I was approached by one of the librarians on the project to develop a more permanent technical solution. I'm a website developer for the OSU Valley Library. Just like most smaller libraries, the Valley Library relies on third-party vendors for many services; however, my department also creates custom web solutions for the library. Because this project required special privacy and security provisions for this vulnerable student population, the library opted for a custom solution.

Determining the Website Goals

First, some risk assessment was needed. This population of users might be constantly worried about a sudden change in status (such as losing DACA status and becoming undocumented), loss of employment, being detained, or being deported to a country where they might not speak the language—all while trying to go to college. That's a lot to worry about.

The users also needed to be able to trust the source of the data. Federal guidance on how to navigate the immigration and DACA system was changing almost weekly and paperwork was taking longer and longer to process. Students would need to be able to access the most recent information quickly.

Students also might not discuss their status and many campus systems are set up deliberately to not collect this information, which is good. However, students might be struggling and no one at the university would ever know. The students needed a safe and reliable way to reach out to advisors who could help them.

Given these conditions, there were two big questions, or goals, for this new website and its data:

- Would students be safe to visit the website?
- Would the resources stay accessible online?

Before I get into specifics, I'm not claiming my solution is keeping all the students' data absolutely safe from any potential threat. That's not possible. My intention is to keep this website from being an access point to vulnerable students by parties outside of the university. Also, I can't share certain information about specific security measures, but I hope to paint a general picture.

Building the Website for Optimal Security

The decision was made to develop and host a website onsite at the library. Everything would be developed by me and hosted on a custom server built by the library's server administrator. The original plan for the site was a basic "pamphlet" site with information about the new Dreaming Beyond Borders resource center, campus DACA and Undocumented policies, a list of advisors who could help, and possibly a blog. Including a blog meant I would need to step up internal security and think hard about passwords and information about registered website editors that would need to store at least a password, a username, and an email address. The blog never happened, but I still made many security and privacy decisions to protect potential website editors.

I decided to use Drupal, an open-source website builder which is similar to WordPress. In this context, "open source" means I can see and edit all the code that the program uses. If the program has code that I don't want, I can delete it. This isn't possible in third-party vendor software being used. For example, Springshare LibGuides is a very convenient website builder, but if I decided I didn't want Springshare to use a particular line of LibGuide code, I wouldn't be able to delete it myself. Additionally, if Springshare were to introduce more invasive tracking into their system, I might never know. This would be true of any closed-source proprietary software or third-party vendor. I wanted to control the code.

I also control the encryption of our Drupal database. Usernames, passwords, emails, and other personal information of content creators are encrypted (basically, scrambled) on the database, so if someone got access to the database, the hacker would not be able to see the personal information. Many data breaches you hear about in the news are just stolen databases in which a company stored personal information in a database without encryption. If a hacker

accessed the database, they could get the contact information of the website editors, which could include DACA and undocumented students who added content to the site.

Hosting the Website Internally for Accessibility and Control

The Valley Library hosts the website internally. Most campus websites are hosted in a centralized location. However, opting for extreme privacy, this site was not to be on any third-party cloud hosting providers such as Amazon Web Services or Acquia, a popular Drupal hosting provider. "Cloud" is just a fancy name for "someone else's servers," rather like how a rented storage unit is basically "someone else's garage." The cloud and storage units often have features you don't have at home, but at the end of the day, you're just a tenant. A hosting provider is able to see what websites are hosted on their platform and can decide whether or not it wishes to host it. This can make the news when big websites are removed by their hosting provider for hate speech or violence, such as when Parler was booted off of Amazon Web Services (Hern, 2021), but hosting companies also ban websites that have illegal content. Acquia specifically bans "Illegal, Harmful or Fraudulent Activities" (Acquia, Inc., n.d.) and DACA could have been considered a legal gray area. Hosting services can also ban sites just because they don't want to host the content. There might not be a reason. Sometimes they even monitor the sites on their platform. A goal for this site was to keep it "live" for as long as possible and to control any monitoring.

Avoiding Data Collection and Profile Mapping

The site was to look and feel like all other official university websites. To this end, the official Oregon State University website theme was used, but without integration with Google Analytics. Google Analytics can be very useful for developers and site owners to get a sense of the user behavior on the site, but it also builds a profile of each user, such as personal interests, hobbies, and political leanings based on their search and browsing history (Google, 2021). Google collects data indiscriminately, so I didn't want to hand Google information about visitors to this site. Again, my intention is to keep this website from being an access point to vulnerable students by parties outside of the university. Also, I didn't really need to know much about who was accessing my site. I knew I could just check with the resource center to learn if users found the layout confusing.

I also removed integration with the Oregon State University's centralized Profiles data. When students logged in to update the site, they were not connected to their centralized university profile.

Ensuring Security and Privacy with https

Finally, the https secure protocol was enforced everywhere on the site. If you're looking for the bare minimum for security and privacy for your own sites, insist on https rather than just http for your website. The "s" stands for "secure." The use of the https secure protocol protects information that travels over the internet, even from your internet service provider. Without https, your internet activity can be seen by anyone with access to your network, such as your internet service provider, your IT person, or anyone else using your same Wi-Fi network. Your internet activity includes email messages, email addresses, passwords, searches, URLs, form content, and so on. Https stops strangers and internet companies from easily scraping your data.

Meeting the Website Safety and Accessibility Goals

So let's think back to the original questions.

Would students be safe to visit the site? The site (https://undocumented.oregonstate.edu) looks identical, on the surface, to other websites across the university, but behind the scenes, every aspect of the website is controlled by the library's small team of developers. I can see all the code and I know what the site does from top to bottom. It is also hosted on the Valley Library's own on-site servers. There's no cloud in which someone else could boot the site off the internet. There are no mystery services that provide minimal functionality for the right to "datamine" visitors. The site is disconnected from third-party providers and has standard modifications for extra security.

Would the resources stay accessible online? As long as the library wants to host the site, it will remain accessible to students. From a legal standpoint, Oregon State University is in Benton County, Oregon, which is a sanctuary county, so it is unlikely that there would ever be local laws against providing information to DACA and undocumented students (Benton County, 2016).

From a technical standpoint, there's always a slim chance that certain kinds of hacks could take the site offline. Contingency plans are in place for if that ever became a problem. Unfortunately, those plans would involve temporary involvement from third-party software, which might slightly undermine the site's safety goal. In that case, the plan includes adding a statement explaining the situation and probably a Warrant Canary, that is, a message which informs students that we have *not* received a subpoena or request for data (Wikipedia, 2021). Luckily, it hasn't come up.

Libraries need usage metrics and assessment data, but you also don't want to open the door to let others mindlessly mine your students' data. This is a delicate balance. Assess the risks for the student population you're serving. Make an intentional choice before you start. Think hard about the kinds of data you need and the data you don't want others to have. As in library responses to the Patriot Act, libraries can't turn over information that doesn't exist. At the very least, make sure you have https on all of your sites.

References

Acquia, Inc. (n.d.). *Acquia acceptable use policy*. https://www.acquia.com/about-us/legal/acquia-acceptable-use-policy

Benton County. (2016, December 20). Commissioners declare "Sanctuary County." *Board of Commissioners Office*. https://tinyurl.com/2p9dkske

Google. (2021). About demographics and interests: Analyze users by age, gender, and interest categories. *Analytics Help*. *https://tinyurl.com/ywcy7pxw*

Hern, A. (2021, January 11). Parler goes offline after Amazon drops it due to 'violent content.' *The Guardian.* https://tinyurl.com/2p8jacwz

Warrant canary. (2021, November 16). In *Wikipedia*. https://en.wikipedia.org/wiki/Warrant_canary

Licensing Online Content to Ensure Patron Privacy:
An Informal Survey of Oregon Librarians

by Jill Emery
(she/her)
Collection Development & Management Librarian, Portland State University Library
jemery@pdx.edu
@jillemery

Jill Emery (she/her) is the Collection Development & Management Librarian at Portland State University Library and has more than 20 years of academic library experience. She has held leadership positions in the American Library Association's Acquisitions Library Collections & Technical Services Division (now known as CORE), Electronic Resources & Libraries, and NASIG. She serves on the Project COUNTER Executive Committee, the Operations and Collections Council of the Western Storage Trust of the California Digital Library and on the advisory committee of the Open Access E-Book Usage project. Jill is a member of *The Charleston Advisor* editorial board and is the columnist for "Heard on the Net," and is on the editorial boards for Collaborative Librarianship and for *Insights: the UKSG journal.* Her co-authored book is *Techniques for Electronic Resource Management: TERMS and the Transition to Open.*

Introduction

Librarians throughout Oregon are committed to securing the rights for patrons utilizing resources within their libraries with the greatest level of protection regarding their online identities as possible. At the same time, Oregon librarians are committed to providing their patrons with the online resources they want to access whether it is a public library, an academic library, a community college library, or a health services library. Finding the balance between providing the desired online content with the safeguards that protect their patrons can be difficult. Oregon librarians recognize the need to secure patrons' online privacy but also want to meet patron demands for resources. Patrons tend to prioritize their quest for content over their personal privacy concerns. By contrast, librarians evaluate the privacy needs of their community as a whole as opposed to on an individual level. They are committed to the third principle of the American Library Association's Code of Ethics: "We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted" (ALA, 2021).

As with many issues in the 21st century, a tension exists between the individual's wants and the best practices for community well-being. To better understand this inherent conflict between access and security, I asked several Oregon librarians to answer a series of questions about their electronic resource licensing practices. This article outlines the current practices these colleagues employ to reconcile this tension between patron demand and patron safety and to identify ways for improving the situation regarding online resource usage.

Methodology

To gather information about electronic resource licensing practices, I contacted librarians working in collection development and management at various Oregon libraries. I did not seek institutional review board (IRB) approval from Portland State University because I was asking about the process and procedure used at their local institutions, and not about how Oregon librarians' feel about the process or practice they were employing. All survey respondents asked to remain anonymous, so throughout this article they are identified only by the type of library they represent.

Annotated Bibliography

- While patron privacy is a topic of great interest to the field of librarianship, it is still an emerging field of study. A rudimentary literature search in *Library, Information Science & Technology Abstracts* (LISTA) revealed the following related works: "Issues in E-resources Authentication and Authorization" (Corrado, 2020) focuses on how patrons access online content, but does not fully delve into the issue of online identity security that can occur with electronic resource usage.

- *Hidden Online Surveillance: What Librarians Should Know to Protect Their Own Privacy and That of Their Patrons* (Fortier & Burkell, 2015) describes breaches of patron information privacy that occur through behavior tracking on provider websites.

- *Licensing Privacy—Vendor Contract and Policy Rubric* (LDH Consulting, 2021) is a presentation given by Becky Yoose on evaluating library licensing agreements for key components on data privacy. This event highlighted a rubric to use when assessing provider agreements for specific clauses regarding patron privacy, confidentiality of patron identification, patron access and use of the resource, and use of patron data.

Licensing Best Practices from Orbis Cascade Alliance

The survey questions for each email respondent were derived from *Licensing Best Practices for Orbis Cascade Alliance & Member Institutions* (Orbis Cascade Alliance, 2020). All Oregon librarians have access to this document, which can be used as a basis for negotiating with vendors on a number of contractual clauses. The privacy clause in this document is considered a required element of all Alliance-negotiated agreements and is comprehensive in its scope and purpose:

> Licensor shall not, without the prior written consent of the Licensee(s) transfer any personal information of any Authorized Users to any non-affiliated third party or use it for any purpose except as is necessary to perform the Services in compliance with applicable State & Federal laws and institutional regulations, including the Family Educational Rights and Privacy Act ("FERPA").
>
> Licensor agrees to maintain the confidentiality of any personal identification data relating to the usage of the Licensed Materials by Licensee(s) and its Authorized Users. Such data may be used solely for purposes directly related to the Licensed Materials and may only be provided to third parties in aggregate form. Raw usage

data, including but not limited to information relating to the identity of specific users and/or uses, shall not be provided to any third party. Vendor will maintain current data security management practices that follow established standards and will notify Licensee in the event of any data breach occurring.

Survey Questions and Responses

Responding to this survey were a public librarian, an academic librarian, a health sciences librarian, and a community college librarian. Each librarian participating in the email survey was asked the same five questions. The following are the questions and a summary of the answers.

1. Do you routinely negotiate review clauses regarding end-user privacy and/or add in a clause regarding end-user privacy in electronic resource agreements?

   The respondents provided similar answers. The community college respondent noted that their information technology office reviews agreements for privacy concerns but if an agreement does not have a clause, they do not insert one. Everyone answered that they review the clause if it is present, but most choose not to negotiate it unless it is seen as stating something egregious or out of line with standard electronic resource usage. The lack of inserting a clause when one is absent was echoed by the academic respondent, public library respondent, and health sciences respondent.

2. If you do actively review agreements for end-user privacy, what in particular are you most concerned with ensuring is included or excluded in regards to a privacy clause?

   When the respondents looked specifically at the privacy clause, the consensus among each respondent was that they focused on patron identification information only being used to enhance the experience with that resource and not collected and distributed elsewhere (to a third party). One respondent noted that they also review resources to see if there are any situations in which a patron can gain additional functionality only by creating an individual account. In such cases, the respondent said they push back on the provider.

3. If you are a member of the Orbis Cascade Alliance, do you actively use the required privacy clause provided by the Licensing Best Practices (Orbis Cascade Alliance, 2020) documentation in local or institutional licensing work?

   Not everyone responding was a member of the Orbis Cascade Alliance, but of those who were, the decision to rely on the best practices was split. There did seem to be familiarity with the best practices but the language provided was not always used readily in negotiation.

4. If you are an Alliance member and do not use the documentation provided in the Licensing Best Practices, can you share why not?

   The reasons why the best practices were not used ranged from there not being a new agreement to negotiate, not having staffing to review past agreements, or that license agreements were managed by procurement or contracts offices where the librarians are not afforded much influence or control over how agreements are handled locally.

5. Lastly, would you be willing not to license a product or service due to a privacy clause to which you felt your library could not agree with or when a provider chose to remain silent on privacy (such as not including a clause at all)?

   The majority of the respondents stated that they had not canceled online resources due to a lack of a privacy clause or because a provider had knowingly used patron information in an inappropriate way. In spirit, they all felt they would cancel if this became an obvious violation of patron privacy. However, most noted that patron desire to have specific content available was the overriding factor for maintaining agreements and content where privacy assurance was dubious. One respondent did note they had canceled a resource after the provider began an aggressive direct marketing campaign to their end users. However, this librarian also noted that their institution made sure to educate end users on the pitfalls of creating personalized accounts with providers through any given providers' website as another way to counter privacy concerns.

Conclusion

Given the responses to the survey, the Oregon librarians who were interviewed are aware of the concerns and potential pitfalls with not signing license agreements for content with problematic privacy clauses or no privacy clauses in place. The demand for content by patrons tends to outweigh concerns of patron privacy. So in this sense, the individual's desire to have content overshadows the work to be done for the common good.

In addition, depending on the institution, the library might not have the final say regarding patron privacy issues. An organization might assign contract negotiation to a procurement office, a contracts committee, or information technology department. In such cases, it can be difficult for librarians to provide meaningful input on the wording of the license agreement. All respondents felt that given the time constraints of their jobs and the myriad of work they are committed to accomplishing daily, undertaking a systematic review of all past license agreements appears to be daunting and an unachievable goal.

The Oregon librarians who participated in the survey appear to be doing the best they can to safeguard patron privacy through their license agreements. They seem to be aware of the best practices available for reference and there is an understanding that patron privacy is a key issue of concern. When trying to balance patrons' desires for content with patron privacy, the best course of action may be in informing the end user of their own responsibility with providing personal information to content providers. While there is an inclination towards wanting to re-review and apply a rubric review such as the one designed by Becky Yoose, the heavy responsibilities of daily activities make this work more aspirational than

practical. As with many issues and concerns within today's libraries, the reconciliation of personal patron need for content versus the work to ensure that the community good is upheld falls back to the best efforts of transparency on behalf of everyone involved and what can be realistically achieved.

References

American Library Association. (2021). *Professional ethics*. http://www.ala.org/tools/ethics

Corrado, E. M. (2020). Issues in e-resources authentication and authorization. *Technical Services Quarterly, 37(*3), 302–314. http://doi.org/10.1080/07317131.2020.1768704

Fortier, A., & Burkell, J. (2015). Hidden online surveillance: What librarians should know to protect their own privacy and that of their patrons. *Information Technology and Libraries, 34*(3), 59-72. https://doi.org/10.6017/ital.v34i3.5495

LDH Consulting Services. (2021). Licensing privacy—Vendor contract and policy rubric. https://tinyurl.com/37rd8vve

Orbis Cascade Alliance. (2020). Licensing best practices for Orbis Cascade Alliance & member institutions. https://tinyurl.com/4dpjhzp7

Student Data Privacy and Automatic Textbook Billing

by Tina Weyland
(she/her)
Reference & Instruction Librarian, Rogue Community College
tweyland@roguecc.edu

Tina Weyland (she/her) is a Reference and Instruction Librarian at Rogue Community College and is a member of the college's Textbook Affordability Group.

The textbook market in U.S. higher education is changing. In recent years, publishers have developed an automatic billing model, in which colleges and universities negotiate deals with publishers to provide ebooks and courseware to students, folding the cost into student fees. This model is commonly known as "inclusive access." Because it offers students first-day access to course materials—important to student success—as well as some savings over full-priced standard textbooks, it is becoming popular with faculty and administrators. But textbook publishers are promoting these plans for another reason: The data they can collect with digital materials opens a lucrative new market, allowing them to diversify into analytics services.

Publishers' textbook revenues have been hurt in recent years by the resale marketplace, Open Educational Resource (OER) adoptions, and lower enrollments. Shifting to automatically collected access code fees allows publishers to recoup some of those earnings, as "inclusive access" contracts provide a higher sell-through rate per course (Aspesi et al, p. 36). Students aren't able to save money in traditional ways—for example, buying used books or older editions, renting, sharing, using library reserves, or selling books back—and publishers likely gain revenue overall. Some educators are pushing back against automatic billing, and not only for cost reasons. Students usually don't retain access to materials after a course ends, and if they need to drop and take a course later, they will be charged again. The contracts can include high quotas for student purchasing and uncapped annual price increases (Vitez, 2020, p. 11).

But as important as these concerns are, the considerable student data these plans allow publishers to capture, as well as the lack of any real option for students who would prefer to protect their privacy, is just as troubling.

> Students can only opt out of this data collection by opting out of the purchase. They are essentially a captive market.

> Once students transition to digital materials it enables both their institutions and the commercial vendors to collect vast amounts of data on them: their physical location when they use them, their study habits, their learning profile, and granular knowledge on their performance. (Aspesi et al, p. 40)

Students can only opt out of this data collection by opting out of the purchase. They are essentially a captive market. While they can sometimes find another way to access the textbook, if they need to submit assignments or take quizzes through bundled courseware, opting out could mean trading a portion of their grade for data privacy. Students do forgo textbooks because of the expense (in a recent study, 63 percent of students had skipped buying for this reason [Nagle & Vitez, 2020]), but with courseware, opting out—for cost or privacy reasons—could mean accepting a lower grade before the course even begins.

Publishing companies are quickly moving toward services that allow them to collect data. Pearson, one of the largest college textbook publishers (Pearson, Cengage, and McGraw Hill together hold 80 percent of the market [Vitez, 2020, p. 1]), has announced it is moving to a "digital first" model in the U.S. (McKenzie, 2019b), and Cengage is aggressively marketing its digital library (Aspesi et al, p. 46). Pearson and Cengage have also developed mobile apps for their content which, while helpful for students without reliable access to a device other than their smartphone, also allow substantial data harvesting.

Institutions should be concerned about what these plans expose their students to—vulnerability to breaches, potential sale of data to third parties, or data being surrendered to governmental authorities, like local police or Immigration and Customs Enforcement (ICE), without judicial process. "The collection of massive amounts of data about faculty and students poses a significant legal and reputational risk for institutions, along with potential privacy and security threats for individuals" (Aspesi et al, p. 8).

This automatic billing model, sometimes presented as an equity solution to the high cost of commercial textbooks, may in fact amplify existing disparities. Publishers tout the convenience of getting materials directly to students; however, this is true only for students with reliable devices and internet connectivity. But, publishers' data collection is its own equity concern. Learning analytics products promise improved student learning through data collection and proprietary algorithms. But algorithms carry the biases of their designers, and can reinforce existing disparities. In one example, COMPAS, an assessment program used to predict prisoners' risk of reoffending, predicted that Black defendants would reoffend more often than they did, and that White defendants were less likely to reoffend than actually occurred (Angwin et al, 2016). And, when the Apple Card was launched by Goldman Sachs, it reportedly offered lower credit limits to women (Vigdor, 2019). The company insisted that a person's gender was not one of its data inputs. But just as neighborhood can be a proxy for race, shopping history might be a proxy for gender. While companies may believe that their (proprietary, secret) algorithms are not considering prohibited characteristics, both the data and the algorithms reflect society.

It is likely that publishers' products could profile students in similar ways. Could student performance data be sold to potential employers, with both the products and their baked-in algorithmic biases entirely hidden from students? While the data collected by publishers may be de-identified, "it could be matched with other third-party databases, leading some to worry that assigning access codes is tantamount to signing students up for surveillance" (Nagle & Vitez, 2020, p. 9).

Best Practices

Students included in automatic-billing plans should be clearly informed, optimally by their instructor, about the data collection allowed. Terms of use should be viewable by faculty and students before sign-up. Plans should be opt-in, but where contracts are opt-out students should receive repeated reminders (through more than one channel) of opt-out dates. Students should be able to meet all course requirements without opting in. And, institutions must consider the unintended consequences of using publishers' automatic billing plans for course materials.
The Scholarly Publishing and Academic Resources Coalition (SPARC) suggests the following risk mitigation measures in negotiating contracts:

- The sale of data to third parties should be prohibited.
- Contracts should prohibit the surrender of students' data to authorities without judicial review.
- Institutions should maintain ownership of collected data.
- The procurement process should be open—no nondisclosure agreements.
- Contracts should require that algorithms using student data be "fully transparent" (Aspesi et al, p. 53).

Students don't know how much data is being collected about them. Surveyed about their knowledge of vendors' data collection, most students rated their understanding at the low end on a scale of 1-10 ("10 being fully aware and able to explain to a peer"), with a median rating of 2 (Nagle & Vitez, 2020, p. 3). Students do need to click through end-user license agreements to access their materials, but the agreements are long and complex, and clicking through is routine for most people. Most of us make decisions about which entities we find trustworthy, but for students who need an assigned textbook, it is not really a choice. Not agreeing to publishers' terms may mean not having what they need to be successful in a course.

Terms of use often include everything and the kitchen sink, as far as what companies are allowed to do.

> Generally speaking, it is standard for terms of use for digital products to include a clause allowing the provider to change terms at any time without notice, possibly retroactively. Faced with increasing financial pressures and tempting opportunities to monetize data, could publishers resist? (Aspesi et al, p. 49)

Further, contract language may give publishers "the option to veto language in institutional communications that give students more context and information" (Vitez, 2020, p. 9). A recent study found that 42 percent of the 31 institutions reviewed "had signed at least one contract that appears to give a publisher final say on any public communications about the automatic billing program."

Resources

Open Oregon's Course Materials Adoption Best Practices—
checklists for administrators, faculty, and students
https://tinyurl.com/mrx87nz9

SPARC information page
www.inclusiveaccess.org

SPARC Automatic Textbook Billing Contract Library
https://tinyurl.com/yc3pn2by

Protecting Student Privacy While Using Online Educational Services:
Model Terms of Service, from the U.S. Department of Education's
Privacy Technical Assistance Center
https://tinyurl.com/35nh3s6a

While federal law requires that publishers' automatic billing plans allow students to opt out, this has its own equity implications for publisher analytics. Opt-in/opt-out frameworks are affected by consent bias, so any products built on the resulting data will be skewed. Those who opt out "may differ systematically, such that the conclusions or actions taken based on the data will unfairly bias one of the groups of students" (Brooks, 2021). A 2019 survey at the University of Michigan, for example, showed that women as a group may be more likely to opt in, with Black students as a group more often opting out (Li et al, 2021).

Most students trust their colleges and assume they have an ethic of care, but this ethic is compromised if decision makers are not considering potential harms. Administrators and instructors seem often to be choosing these plans while unaware about the data collection piece. Many institutions likely need to take a more comprehensive approach to data collection in general, with a wider set of stakeholders (faculty, librarians, staff, and students) included in decision-making. "Policies governing student data collection and use have lagged behind technological and cultural changes in higher education" (Brown & Klein, 2020, p. 4).

The Family Educational Rights and Privacy Act (FERPA) does not prevent data exploitation by publishers; constraints apply only to educational institutions, not vendors or other third parties. Passed in 1974, the act is commonly viewed as preventing institutional disclosure of student data. However, the law was originally motivated not by worries over improper disclosure, but by the impact of the data collection itself on students' lives—concern about "secret gatekeepers, arbitrary categorizations, and bureaucratic errors that, unchecked, could become permanent liability" (Igo, 2018, p. 250). Lawmakers worried that "inaccurate information or biased judgements about students would linger … creating a 'records prison' that follows students" (Brown & Klein, 2020, p. 5).

> At issue was not so much whether a pupil would be documented in a variety of ways … but whether that student's record would be documented accurately and fairly, how long it would be maintained, who else would have access to it, and how the subject of that record would go about finding out what it contained (Igo, 2018, p. 250).

Protecting user privacy is one of librarians' core values. Most higher education institutions in Oregon have librarians working on textbook issues, and librarians should be advocating within their institutions for students' data privacy interests. Librarians have an important role to play in helping students, faculty, and administrators understand how this data is being collected and how it might be used. As Nicole Allen of the Scholarly Publishing and Academic Resources Coalition (SPARC) said of automatic billing plans, "Higher education owes it to students to grapple with the ethics of this new course content landscape" (McKenzie, 2019).

References

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016, May 23). Machine bias. *ProPublica*. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Aspesi, C., Allen, N. S., Crow, R., Daugherty, S., Joseph, H., McArthur, J. T., & Shockey, N. (2019, March 29). *SPARC landscape analysis: The changing academic publishing industry—implications for academic institutions*. https://doi.org/10.31229/osf.io/58yhb

Brooks, C. (2021, September 20). Privacy opt-out may lead to inequities. *Inside Higher Ed.* https://tinyurl.com/yc7rmnxp

Brown, M., & Klein, C. (2020). *Whose data? Which rights? Whose power? A policy discourse analysis of student privacy policy documents.* Iowa State University Digital Repository. https://dr.lib.iastate.edu/handle/20.500.12876/104715

Igo, S. E. (2018). *The known citizen.* Harvard University Press.

Li, W., Sun, K., Schaub, F., & Brooks, C. (2021). Disparities in students' propensity to consent to learning analytics. *International Journal of Artificial Intelligence in Education,* 1–45.

McKenzie, L. (2019a, April 26). Scrutiny of a financial relationship. *Inside Higher Ed.* https://tinyurl.com/2p85nwpe

McKenzie, L. (2019b, July 16). Pearson's next chapter. *Inside Higher Ed.* https://tinyurl.com/3hx86nkk

Nagle, C., & Vitez, K. (2020). *Fixing the broken textbook market* (2nd ed.). U.S. PIRG Education Fund.

Vigdor, N. (2019, November 10). Apple Card investigated after gender discrimination complaints. *New York Times*. https://tinyurl.com/mwcpu8cp

Vitez, K. (2020). *Automatic textbooks billing: An offer students can't refuse?* https://tinyurl.com/2b737yjx

The Distance Between Our Values and Actions:
We Can't Be Passive When it Comes to Privacy

by Meredith Farkas
(she/her)
Faculty Librarian,
Portland Community College
meredith.farkas@pcc.edu
@librarianmer

Meredith Farkas (she/her) is a Faculty Librarian at Portland Community College, a proud member of the Library Freedom Project, a perpetual beginner, and a recovering workaholic. From 2007–2021, she wrote the "In Practice" column for *American Libraries* and has also authored the blog *Information Wants to be Free* since 2004. Meredith was honored in 2009 with the LITA/Library Hi Tech award for Outstanding Communication in Library and Information Technology, and in 2014 with the Association of College and Research Libraries Instruction Section Innovation Award. She has held many different leadership and management roles in her career, but her favorite is working with students and faculty as an instruction librarian.

In September 2021, the WOC+Lib collective published a searing "Statement Against White Appropriation of Black, Indigenous, and People of Color's Labor (BIPOC)," decrying the exploitation and abuse of BIPOC library workers. One of the many hypocrisies the group took issue with was:

> the proliferation of anti-racism statements put out by information institutions and organizations in 2020 without also taking on actions addressing the lack of Black, Indigenous, or People of Color workers or how the BIPOC within those very libraries and organizations have been ostracised and disrespected for years prior to 2020, while allowing the mistreatment to continue. (WOC+Lib, 2021)

In the midst of the international uprisings for racial justice following the murder of George Floyd, many libraries put out antiracist statements affirming their commitment to diversity, equity, and inclusion (DEI). Yet in a recent survey of library directors, only 31 percent of academic library directors agreed that their "library has well-developed equity, diversity, inclusion, and accessibility strategies for employees" (Frederick and Wolff-Eisenberg, 2021, p. 10). The lack of progress made in these areas suggests that while diversity may be a library value, dismantling systems of oppression to improve DEI is not a top priority at most institutions.

When we are acting in ways counter to one stated value, there is usually another value or power structure influencing that choice.

In "On the Disparity Between What We Say and What We Do in Libraries" (2017), Baharak Yousefi explores the distance that often exists between our stated commitments and our actions in libraries. She finds that libraries frequently take action or fail to take action in ways that run directly counter to our stated values. In trying to understand the forces at work in these choices, she suggests that "our actions are also influenced by de facto forms of power that are often more consequential than our official positions" (p. 93). When we are acting in ways counter to one stated value, there is usually another value or power structure influencing that choice. So a library that puts out an antiracist statement and then does nothing substantive to address these issues in their own institution is likely prioritizing other things, like neutrality or the desire to avoid conversations that make White people uncomfortable. The key, though, is recognizing that an active choice is always being made that reflects the values and power structures that are really driving us.

Words vs Deeds in Library Patron Privacy Rights

The parallels between our commitment to DEI and our commitment to privacy are striking. The importance of protecting patron privacy is enshrined in the Library Bill of Rights and the American Library Association's (ALA) Code of Ethics. The ALA Core Values of Librarianship states that "protecting user privacy and confidentiality is necessary for intellectual freedom and fundamental to the ethics and practice of librarianship" (American Library Association, 2019). In addition to our commitment to protecting patron privacy in our work, library workers and the ALA have a long history of protesting government spying and other forms of surveillance that iFmpact members of their community. Our professional community venerated the Connecticut Four who resisted the FBI and took the Justice Department to court over the Patriot Act (SinhaRoy, 2021). Yet in our current information ecosystem, few libraries, if any, can claim that they ensure the privacy of their patrons.

The growth of digital collections, analytics, and social media has challenged our commitment to privacy. This is a result of both the complexity of the information environment as well as a desire to capitalize on new technologies and information sources to better understand our patrons, market ourselves, or demonstrate value. Many librarians are unaware of the extent to which their vendors violate the privacy of their patrons and lack the skills or access to understand what vendors are doing with patron data (Nichols Hess et al., 2015). In other libraries, neoliberal pressures from parent institutions have led libraries to adopt practices that are common among technology companies but not consonant with our stated values around privacy.

Third-Party Trackers from Publishers and Databases Can Harm Our Patrons

There are many reasons why library workers should be concerned about the practices of the publishers and database vendors we fund. Most concerning to me was the research of Cody Hanson (2019) at the University of Minnesota who found that 14 of the 15 publisher platforms he examined included third-party trackers in their product's code. Many of these trackers allow third parties to view patron actions in the platform—searches, articles accessed, and so on—and, in some cases, to associate those actions with an existing individual profile (Facebook, Google, etc.). Even without a cookie that reveals their identity, third-party trackers often collect enough information about a user and their web browser through browser fingerprinting to identify them. This means these third-party apps can often reveal

a user's identity and add what they are doing on the publisher platform to the growing profile data brokers have about each of us. Data brokers develop profiles of individuals' online behavior to sell those profiles to various companies and people. Hanson rightly recognizes that the information being collected by these third-party trackers is the same type of patron information that the Connecticut Four went to court to protect from the FBI, yet a recent study by Licensing Privacy found that for library leaders "the issue of privacy does not take precedence in negotiating licenses" (Cooper, 2021).

There are very real potential harms to our patrons from their library data being incorporated into the surveillance economy. Given that surveillance regimes tend to have the greatest negative impact on BIPOC (Cyril, 2015), the largest harms will likely be felt by our most marginalized patrons. Some library vendors, like LexisNexis and Thomson Reuters, already act as data brokers for the U.S. Immigration and Customs Enforcement (ICE) and other law enforcement agencies and both "modified their privacy statements [in 2018] to clarify that they use personal data across their platforms, with business partners, and with third party service providers" (Lamdan, 2019). We've seen police and prosecutors use social media to identify, arrest, and prosecute protestors (Iboshi, 2021), so it's not a reach to imagine patron data being used to identify suspects, establish intent, or even be incorporated into big data systems that determine things like bail and sentencing (Angwin, 2016). It's also not a stretch to imagine health-related searching being used by insurance companies as many have contracts with data brokers (Sherman, 2021). My family recently started seeing ads on Hulu for a pill treating a very rare condition a member of our family has, clearly targeted to people who search for information on that condition. If information like that can be shared with drug companies and streaming providers, why not insurance companies and current or potential employers?

Libraries can make the argument that they have limited ability to impact the practices of vendors, but the same cannot be said for other choices libraries make that compromise their patrons' privacy. In 2013, I wrote in this journal about my concern with the move—after the publication of the *Value of Academic Libraries* report (Oakleaf, 2010)—away from assessment focused on improvement toward a focus on demonstrating the value of the library (Farkas, 2013). When I attended the Library Assessment Conference in 2014, the focus of the keynote speeches and many other presentations was on collecting transaction-level data tied to patron identity in order to demonstrate value, provide targeted interventions to different student populations, and "deliver the sort of personalized and responsive user experience that has become an expectation of online citizens" (Kay, 2014, p. 273). One keynote speaker argued that even if we don't yet know how we are going to use the data, we should immediately begin collecting "atomic activity data" from every library system (p. 280). What was missing from all of these presentations was *any* discussion of privacy.

The Problem with Learning and Library Analytics for Measuring Outcomes

In the ensuing years, the encroachment of neoliberal values in higher education has increased along with the use of transaction-level data by libraries to demonstrate they are a good investment and contribute to the goals of the college or university. Many libraries are using student data to show that use of the library (like checking out books, searching in a database, or asking a reference question) is tied to higher academic achievement (Jones et al., 2020). Of those libraries that are using patron-level data in this way, exceedingly few fully de-identify student data or have edited their privacy policies or statements to account for this work (Perry et al.,

Just because we can easily and invisibly do something, doesn't mean we should.

2018). Some libraries now include library usage data in college or university-wide learning analytics systems. Learning analytics systems collect data about students from many different online platforms in order to illuminate patterns or trends and suggest interventions to improve student success. These systems, by looking at academic achievement across classes, can predict ideal paths through the curriculum for different groups of students. Some of these systems alert advisors or faculty members when the data on a particular student suggests they might be struggling. Other systems actually "'nudge' students toward certain behaviors, such as communicating with instructors or seeking campus resources, based on these predictions" (Jones et al., 2020, p. 572). In libraries, analytics data could allow libraries to personalize their services and identify students for outreach efforts.

Collecting and keeping large amounts of transaction-level data tied to student IDs or even demographic characteristics can help us learn a lot about our patrons, how our resources and services are used, and their impact, but the question remains whether we should collect this data if we are not also committed to the de-identification of that data. Use of the library isn't like taking a class, which is part of one's educational record. It should be no one's business but the patron's whether or not they used the library and what resources they consulted. There are many other behavioral data points that would help us improve a student's educational experience, but we don't collect that data because it would be difficult or intrusive. Just because we can easily and invisibly do something, doesn't mean we should. What's more, when we put library data into learning analytics or predictive analytics systems, we are giving access to individuals across the college or university who may not share the library's commitment to student privacy. We not only lose control over how that information might be used, but by retaining that data, we increase the risk of the information being exposed in data breaches, which have become common. Also, it doesn't take much imagination to see some higher education institutions' use of learning analytics going the way of a dystopian *Black Mirror* episode.

Given that many colleges and universities have swipe card systems that feed into their learning analytics tools, I could imagine a system that looks at everything a student does on campus and shares it with their instructors and advisors so they can advise the student on the "right path" (likely based on Whiteness norms) for them without ever needing to get to know the student. The University of Wollongong's Library Cube project—originally designed to demonstrate library value—provides patron usage data to their institution's learning analytics system, which then can alert instructors if a student's library use is concerning (Jantti, 2014). I can imagine instructors grading students based on library use or other behavioral data collected that has nothing to do with their coursework or participation. Already some instructors have sought to grade students based upon the amount of time they spend in their online classroom (Grading Students On Time Spent In The Course, 2014).

If a system can uncover ideal paths for student success and identify students who are in danger of failing, it can predict which students are less likely to be successful before they even start college. Given the racial disparities in success rates across higher education (Libassi, 2018), this could lead to the exclusion of students from already underrepresented groups. In light of the current economic outlook in higher education and news about the

closures of numerous institutions, economic interests might trump a focus on increasing diversity or even a duty of care at some institutions. Hundreds of universities already use a predictive analytics product that is far more likely to assign a high risk score for not succeeding in college to Black and Latinx students (Swauger, 2021).

Advocates for library analytics argue that libraries don't have a choice but to engage in these practices in an age of increased austerity and questions about the relevance of libraries. Cox and Jantti (2012) argue that "libraries that do not provide such evidence will be at an increasing risk of having their funding reduced or eliminated" (p. 309). However, data connecting library use to student success is correlational, not causational, and going to the gym, having a part-time job, and living on-campus have also been correlated with better student outcomes (Farkas, 2018), so it's questionable how meaningful it is to demonstrate this connection. It would be lovely if we could really distill the impact of library collections and services on our patrons, but using the library isn't like taking a pill. We are trying to rationalize and quantify something that is irrational, messy, and mostly unquantifiable; something that is better captured by using qualitative methods that uncover our patron's stories.

Libraries Can Help Patrons Protect Their Privacy Rights

It's unlikely that we will see a groundswell of activism around privacy rights at the scale that we have seen for racial justice, but surveillance capitalism has received increased media attention in recent years and awareness of these issues is growing. What is missing from the cases above is informed consent. Patrons rarely know what data is being collected and only give "consent" in that they use a particular platform. Only 10 percent of papers reporting the results of library analytics projects even mentioned consent at all (Jones et al., 2020). At a minimum, patrons deserve to know what information is collected about them and how it might be used. Ideally, they should be able to opt out of data collection entirely. Allowing this data collection, retention, and use to happen without patrons' knowledge is not only paternalistic, but potentially damaging. When we decide that the ends justify the means in these situations, we are deciding that for all of our patrons, some of whom may be legitimately harmed by the information collected about their library activities. This is in direct opposition to what most patrons expect from a library.

The rhetoric around these issues frequently makes it sound like libraries don't have a choice, but the reality is that, while the choices may be difficult, we do have agency. Library privacy advocates like Becky Yoose (2017) have demonstrated that while protecting patron privacy is time-consuming and requires staff with significant technology skills, it is possible. We could better educate ourselves on these issues in order to make well-informed ethical choices and we could utilize the power of our larger organizations (consortia, associations, and state libraries) and bodies that create standards and regulations to advocate for broader changes. Our current choices suggest that we value providing content and collecting data to show how valuable we are far more than we value protecting our patrons' information.

Libraries are driven by the fear of not being considered valuable or relevant. It's important that we, in our libraries, openly discuss the unspoken assumptions and power structures that lead us to make choices in opposition to our values. We should also consider what privacy rights and agency we feel our patrons deserve and examine how large a gulf exists between that ideal and the current reality. By uncovering the very real power structures and assumptions driving these choices, we can confront them and find new ways to operate that better center our stated values.

References

American Library Association. (2019). Core values of librarianship. *American Library Association*. https://www.ala.org/advocacy/intfreedom/corevalues

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016, May 23). Machine bias. *ProPublica*. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Cooper, D. (2021). *Licensing privacy: Views from library leadership* [Video]. Licensing Privacy. https://mediaspace.illinois.edu/media/t/1_p3wr5apq/235953223

Cox, B. L., & Jantti, M. (2012). Capturing business intelligence required for targeted marketing, demonstrating value, and driving process improvement. *Library & Information Science Research, 34*(4), 308–316. https://doi.org/10.1016/j.lisr.2012.06.002

Cyril, M. A. (2015, March 30). Black America's state of surveillance. *The Progressive Magazine*. https://progressive.org/magazine/black-america-s-state-surveillance-cyril/

Farkas, M. G. (2013). Accountability vs. improvement: Seeking balance in the value of academic libraries initiative. *OLA Quarterly, 19*(1). http://journals3.library.oregonstate.edu/olaq/article/view/vol19_iss1_3

Farkas, M.G. (2018). We can, but should we? When trends challenge our professional values. *American Libraries, 49*(3/4), 46. https://tinyurl.com/2p9hxeau

Frederick, J., & Wolff-Eisenberg, C. (2021). *National movements for racial justice and academic library leadership: Results from the Ithaka S+R US Library Survey 2020*. https://tinyurl.com/2p9y2dmk

Grading students on time spent in the course. (2014). *NROC Project Help Center*. https://tinyurl.com/3c4ksp24

Hanson, C. (2019). User tracking on academic publisher platforms. *Cody Hanson.* https://www.codyh.com/writing/tracking.html

Iboshi, K. (2021, January 13). Portland protest cases provide blueprint for how feds will use social media to arrest Capitol mob. *KGW8*. https://tinyurl.com/mvuk6tkp

Jantti, M. (2014). Aspiring to excellence: Maximising data to sustain, shift and reshape a library for the future. *Proceedings of the 2014 Library Assessment Conference*, 15–22. https://www.libraryassessment.org/wp-content/uploads/bm~doc/proceedings-lac-2014.pdf

Jones, K. M. L., Briney, K. A., Goben, A., Salo, D., Asher, A., & Perry, M. R. (2020). A comprehensive primer to library learning analytics practices, initiatives, and privacy issues. *College & Research Libraries, 81*(3), 570. https://tinyurl.com/mr3uspz4

Kay, D. (2014). Discovering the pattern, discerning the potential: The role of the library in unraveling the cat's cradle of activity data. *Proceedings of the 2014 Library Assessment Conference*, 269–282. https://tinyurl.com/39tx6nse

Lamdan, S. (2019). Librarianship at the crossroads of ICE surveillance. *In the Library with the Lead Pipe*. https://www.inthelibrarywiththeleadpipe.org/2019/ice-surveillance/

Libassi, C. (2018, May 23). *The neglected college race gap: Racial disparities among college completers. Center for American Progress.* https://tinyurl.com/mw29wtmv

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

Oakleaf, M. (2011). *Value of academic libraries: A comprehensive research review and report.* Association of College and Research Libraries. https://acrl.ala.org/value/?page_id=21

Perry, M. R., Briney, K. A., Goben, A., Asher A., Jones, K. M. L., Robertshaw, M. B. & Salo, D. *Learning analytics*. SPEC Kit 360. Washington, DC: Association of Research Libraries, September 2018. https://publications.arl.org/Learning-Analytics-SPEC-Kit-360/

Sherman, J. (2021). *Data brokers and sensitive data on U.S. individuals: Threats to American civil rights, national security, and democracy.* Duke Sanford School for Public Policy. https://tinyurl.com/445euzs4

SinhaRoy, S. (2021, September). Defenders of patron privacy. *American Libraries Magazine.* https://americanlibrariesmagazine.org/2021/09/01/defenders-of-patron-privacy/

Swauger, S. (2021, November 12). The next normal: Algorithms will take over college, from admissions to advising. *Washington Post.* https://tinyurl.com/2p8tc232

WOC+Lib. (2021, September 3). *Statement against white appropriation of Black, Indigenous, and People of Color's labor.* WOC+Lib. https://tinyurl.com/y2rdwy7c

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://journals.ala.org/index.php/jifp/article/view/6250/8393

Yousefi, B. (2017). On the disparity between what we say and what we do in libraries. In S. Lew & B. Yousefi (Eds.), *Feminists among us: Resistance and advocacy in library leadership.* Sacramento, California: Library Juice Press. https://summit.sfu.ca/item/17387

OLA Quarterly Publication

The *OLA Quarterly (OLAQ)* is the official publication of the Oregon Library Association. The *OLAQ* is indexed by *Library Literature & Information Science* and *Library, Information Science & Technology Abstracts.* To view PDFs of issues, visit the OLAQ Archive on the OLA website. Full text is also available through HW Wilson's *Library Literature and Information Science Full Text* and EBSCO Publishing's *Library, Information Science and Technology Abstracts (LISTA) with Full Text.*

Each issue is developed around a theme determined by the Communications Committee and Guest Editor(s). To suggest future topics for the *OLA Quarterly,* or to volunteer/nominate a Guest Editor, contact olaq@olaweb.org.

Oregon Library Association Inc.
PO Box 3067, La Grande, OR 97850

The OLA Communications Committee