Urban Library Journal

Volume 21
Issue 2 *Selected proceedings from the 2015 LACUNY Institute: Privacy and Surveillance: Library Advocacy for the 21st Century.*

Article 4

9-8-2015

The Walled Gardens of Ebook Surveillance: A Brief Set of Arguments Against DRM in Libraries

Alycia Sellie
Graduate Center, CUNY

The Walled Gardens of Ebook Surveillance: A Brief Set of Arguments Against DRM in Libraries

There are three claims I will make in this article about including electronic books with DRM restrictions in library collections. These arguments center upon what the presence of restricted ebooks signifies to patrons about libraries. The first argument outlines how providing books with DRM encourages library users to adopt low expectations for how their personal information will be shared and collected. Second, when users encounter DRM within library collections, not only are they frustrated by the ways that these systems restrict their use of a text, but they become more broadly disappointed in their library. Finally, I will show how the current technological landscape that allows third party surveillance via DRM threatens the professional standing of librarians as protectors of patron information.

What is DRM?

To me, DRM stands for Digital Restrictions Management. But choosing to call it such is a political choice.[1] Others refer to DRM as Digital Rights Management. In a nutshell, DRM controls access to digital content and restricts the functionality a devices, such as an ebook reader or computer. The way that most DRM systems function is by encrypting the files that make up a text in order to strip away what you can do with a file. For example, with ebooks, a DRM system may remove the ability to print, download the full book, copy parts of the text, or retain access to a particular work over time.

DRM is a technical restriction, not a legal restriction.[2] DRM is a system of software and code, not a license or copyright in itself. DRM often is implemented as a form of restriction placed on top of copyrighted works, but DRM could also be applied to ebooks that have alternative or open licenses. I want to stress that DRM and copyright are not synonymous. Further, DRM can also restrict the use of a work even further than standard fair use would legally allow (Lessig, 2006, p.185). DRM can be a way to make the desires of a copyright holder come through into the functionality of a work—regardless of how legal such restrictions might be.

Walled Gardens

[1] Relating DRM to restrictions rather than rights comes from conversations within the free software movement. For more information see Richard Stallman's warnings in the work, "The Right to Read" (2014) and the campaigns of the Defective by Design committee.

[2] The Digital Millennium Copyright Act regulates what can legally be done with DRM software. For more information about this act and its history, see: https://www.eff.org/issues/dmca

DRM is an example of a closed platform, or a walled garden. Walled gardens are set up so that a user has very little ability to navigate within an environment. Using a computer that has access to the internet but is very restricted through content filters is one example of systems like this—you can see a portion of the web, but not the whole. Access is limited and controlled.

Walled gardens exist in contrast to open platforms, in which users could have access to all content and perhaps even be able to examine the code itself that makes up the full environment.

When I think about ebooks and DRM, I imagine that ebook files are shuttled in a very limited way, like a subway train that only can move back and forth on one short track. Ebooks with DRM can only go from one provider (say ebrary) to their chosen platform (i.e. Adobe Digital Editions). Their only possible route is from one station to another, in this limited ecosystem. DRM cages content where open systems allow content to be free range.

DRM makes ebooks have a very restricted life, and these limitations do not allow transformations of digital books that might be of benefit to readers in many varieties of ways. There are many important and legal reasons why one might want to transform a work that DRM might not allow; for issues of sight or hearing and compliance with the Americans with Disabilities Act, to remix a work into something else, to retain a text for reworking, for text mining or big data projects, and the list goes on. DRM makes ebooks rigid and restricted where they could become sites of exploration and discovery.

Another worrisome aspect of this shuttled, walled environment is that DRM makes surveillance of reading habits extremely simple. The same mechanisms that keep ebooks locked within a DRM platform also make it so that whoever is providing the books can see and log patron behavior.

DRM systems that protect content also track patrons. They store more data about readers than libraries have ever collected—not only which books have been checked out, but also what specific pages were viewed, how often, by whom, and from what location. Recent security breaches in Adobe Digital Editions software revealed not only that Adobe was tracking every document in a reader's library through DRM, but also that the Adobe security systems were so lax that they were sharing this data unencrypted over the web in ways that were plainly visible online (Hoffelder, 2014; McSherry, 2014).

Third parties that collect information about reading habits do not share libarians' professional commitments to privacy. When asked by the state or other parties, they are likely to comply with requests for information. By trusting third parties with

patron data, we may never know how much or how often data is shared and with whom.[3]

DRM and Disney

Recently I was reminded of DRM when I was reading comedian Adam Resnick's recent book, *Will Not Attend*. A chapter of Resnick's book talks humorously about how he did not enjoy a visit to Disneyland. Having never been myself, I was intrigued when he described that when a family visits Disney, everyone in the group is given an identifying wristband that is used to pay for the incidental costs of the vacation (2014, p.39).

I immediately felt like this was another important analogy for the way that ebooks with DRM function in libraries. While it might seem like an odd connection, this combination of personal surveillance and restrictive technologies is frighteningly similar. Both are systems that force people to give up information about themselves in order to participate; systems that force an interested person to wear a wristband and be tracked in order to take part, or to go on the rides.

There are many other situations today where corporations use friendly apps, give coupons, or have loyalty programs to get data about their customers—from coffee shop reward programs on smartphones to other offers via online coupons. We don't always think of these offerings as surveillance, but our shopping habits are increasingly tracked for marketing or other purposes by corporations (Schneier, 2015).

In most of these cases, we, as consumers, have a choice. We can easily still buy a latte even if we opt out of using the coffee app. We can politely refuse to be part of a loyalty program. We can pay with cash. We can cover the cameras built into our laptops, use free software, or decide not purchase a cell phone—no one is forcing us to put on a Mickey Mouse bracelet if we would rather not.

Whereas when librarians choose to provide sole access to a text as an ebook with DRM, we have removed any ability for our patrons to choose how and when to share their data. This steering toward surveilled books offers even fewer alternatives when the book in question is held by an academic library and has been assigned to a class for a course, or when a student is expected to have access to a specific device in order to read a restricted text.[4] Essentially, what we are saying to patrons when we

[3] For more information on the dangers of sharing information with third parties, see Kade Crockford's talk, "Privacy in the Age of Dragnet Surveillance: What you Need to Know to Protect Your Rights Online" (2015).

[4] This becomes ever more important as we see more evidence that students use many different devices in research and writing. Increasingly important is the ability to read and write on cell phones and during commutes (and without an internet connection), as Mariana Regalado and Maura

offer no alternatives to DRM restricted ebooks is that if they want access to content, they must allow their reading habits to be surveilled. They must wear a bracelet at all times to participate, or create and use an identifying account every time they would like access to content.

While giving information about how someone reads to a publisher or vendor might not seem as dramatic as protecting other more immediately impactful data, the mere presence of DRM and its surveillances creates a poor relationship between libraries and readers.

Promoting Surveillance

DRM systems encourage patrons to neglect their personal privacy. The inclusion of materials with DRM in library collections signals an endorsement of DRM on the part of libraries and librarians, and likewise, an acceptance of surveillance.

For patrons who assume that libraries are protecting their data, encountering a DRM system might lend a false sense of belief that DRM is safe. They may incorrectly assume that these systems, and their information, is being handled with care by the library alone and not being aggregated by a third party. As Sutlieff and Chelin (2010) studied in England, patrons often expect that libraries are working in the best interests of protecting their privacy, even when they do not have evidence that this is the case—there is a level of trust for libraries that is not often given to other institutions.

By including ebooks with DRM in their collections, librarians misuse this patron trust and contribute to cultures of surveillance. Library catalogs and websites promote metadata surveillance when DRM is part of a library's online presence. The prevalence of DRM creates an increased tolerance for insecure systems, and comfort with the fatalistic notion that surveillance is inevitable. But comfort with sacrificing personal information should not be part of what libraries teach their communities.

The appearance of DRM in library systems says to those who are already protective of their privacy to be wary that libraries are not looking out for their interests. When we use DRM, we lose the trust of those who would rather not identify themselves in order to access content. And we are making it impossible for those who expect to be able to understand how something works to make an informed decision before agreeing to any terms—the secrecy and restrictive nature of walled gardens are a big turn-off for many of our potential patrons.

Smale have shown in their ethnographic studies of commuter students throughout the City University of New York (2015).

DRM and Disappointment

A few years ago, a comic strip was circulating through social media. It depicts the process of downloading an audio book from the Cleveland Public Library. In 22 steps, it walks through what is required, from selecting a book to installing a few forms of proprietary software. Then, a bit more software. Followed by a series of cryptic messages that the user must get through. By step 18, our comic strip's potential audio book listener has broken down into expletives. Step 19 is "Give up on stupid library" (Colbow, 2010).

The title of this comic is "Why DRM Doesn't Work." Patrons are avoiding certain technologies because of the hassles of DRM. When libraries are the institutions known best for using these broken technologies within walled gardens, patrons are avoiding libraries as well.

The practical frustrations that DRM poses, beyond the philosophical, are real and important—how these systems do not operate akin to printed books. In my experience as a librarian I have never had a patron tell me that they adore any ebook platform that uses DRM. I have had droves of patrons who have confessed that they hate ebooks—not because of inherent bad experiences with digital books themselves—but because of the hurdles of trying to navigate DRM.

As librarians, we need to talk more critically about what we are asking our patrons to do in order to read an ebook: what kinds of systems and platforms are we using? What technical expectations do we have for patron privacy? What assumptions are we making about our patrons' machines and devices when we offer them an ebook? Can we convince them that libraries aren't stupid?

DRM Threatens Librarians' Standing as Privacy Advocates

In the Fall of 2014, I attended a conference at New York University that brought together legal scholars, technology activists, and a few librarians. The mission of the conference was to examine whether a technological equivalent could be made for physical signs that activist librarians had created after the USA Patriot Act went into effect. The signs, also known as "warrant canaries," were made in response to the gag orders associated with talking about requests for information associated with the Patriot Act. Displayed in libraries, one example read, "The FBI has not been here [watch very closely for the removal of this sign]" (West, 2009).

For me, this conference showed that we're living in a moment when technology and law experts are looking for allies who uphold privacy. Librarians have a historic connection to promoting intellectual freedom and protecting patron information, and these colleagues want to hear from us.

But if we still shove our patrons onto platforms that will track and sell data about their reading habits, or contain what they can access within walled gardens, then

we are failing to uphold our professional ethics, and we do not have a leg to stand on within these conversations.

If we librarians are known to uphold patron privacy, then we are taking advantage of and violating our own reputations when we purchase and provide books with DRM. Because of the reasons that I have outlined above, when we present only one way to access a book, and that way requires use of a restricted, platform-specific version that tracks reading data and personal information, then we are doing a disservice to our professional ethics as protectors of patron information and champions of intellectual freedom.

There are plenty of things we can do; we are not forced to choose DRM and we should not force our patrons to choose it. We can resist buying products with DRM; we can stick with print or allow patrons to get copies of items that are in our holdings through Interlibrary Loan when they would prefer not to use an ebook (I know that library budgets are ever increasingly cut, but this winnowing is more reason to take care with what we buy). We can become more critical of third parties and insist that they make their polices about data collection and retention clear (and we can apply pressure). We can listen to patron discomfort about ebooks and understand that wariness about the format may not merely be an unwillingness to go digital but might instead correlate to larger issues of privacy and trust.

If librarians want to be a part of future conversations about privacy (and I hope that we do), we have to stop providing and thereby promoting ebooks with digital restrictions.

REFERENCES

Colbow, B. (2010, March). Why DRM Doesn't Work, or, How to Download an Audio Book from the Cleveland Public Library. *The Brads*. Retrieved from: http://www.bradcolbow.com/archive/view/the_brads_why_drm_doesnt_work/?p=205

Crockford, K. (2015 April 16). Privacy in the Age of Dragnet Surveillance: What You Need to Know to Protect Your Rights Online. Conducted from Graduate Center, CUNY, New York. Retrieved from: http://videostreaming.gc.cuny.edu/videos/video/3323/

Defective by Design. (n.d.). Retrieved from: http://www.defectivebydesign.org/

Digital Millennium Copyright Act. (n.d.). Electronic Frontier Foundation. Retrieved from: https://www.eff.org/issues/dmca

Hoffelder, N. (2014, October). Adobe Spying on Users, Collecting Data on their eBook Libraries. The Digital Reader. Retrieved from: http://the-digital-reader.com/2014/10/06/adobe-spying-users-collecting-data-ebook-libraries/

Lessig, L. (2006). *Code 2.0*. New York, NY: Basic Books.

McSherry, C. (2014, October). Adobe Spyware Reveals (Again) the Price of DRM: Your Privacy and Security. *Electronic Frontier Foundation*. Retrieved from: https://www.eff.org/deeplinks/2014/10/adobe-spyware-reveals-again-price-drm-your-privacy-and-security

Regalado, M., and Smale, M. A. (2015). Serving the Commuter College Student in Urban Academic Libraries. Urban Library Journal. Retrieved from http://ojs.gc.cuny.edu/index.php/urbanlibrary/article/download/1619/Serving%20the%20Commuter%20College%20Student%20in%20Urban%20Academic%20Libraries

Resnick, A. (2014). *Will Not Attend: Lively Stories of Detachment*. New York, NY: Penguin Group.

Schneier, D. (2015). *Data and Goliath*. New York, NY: W. W. Norton and Company.

Stallman, R. (2014). The Right to Read. *GNU Operating System*. Retrieved from: https://www.gnu.org/philosophy/right-to-read.html

Sutlieff, L. and Chelin, J. (2010) 'An absolute prerequisite': the importance of user privacy and trust in maintaining academic freedom at the library. Journal of Librarianship and Information Science, 42 (3). pp. 163-177.

West, J. (2009, September). The FBI, and whether they've been here or not. *Librarian.net*. Retrieved from: http://www.librarian.net/stax/4182/the-fbi-and-whether-theyve-been-here-or-not/