Bryan Jones
LFI Week 11
Comparing vendor policies

Below I compare the privacy policies of three popular library services offered by third party vendors: Freegal, Overdrive, and Lynda.com. The first two are services created for libraries, the last is primarily created for businesses or individuals but they also offer institutional accounts to libraries. For brevity, I only consider desktop websites and not the permissions of their mobile apps.

Freegal

https://nashville.freegalmusic.com/privacy-policy

On their homepage, they state prominently that they are compliant with GDPR. The privacy policy itself directly at the top of the homepage with the notice about GDPR.

They assert that though you may be asked to provide personal information for some services; e.g., support inquiries, for normal use they "do not collect any personal information. In general, unless you tell us, we do not know who you are." They do go on to say, "We may also use personal information in the course of data analysis to help us improve our products, services, and operations. **Personal information will not be shared by Library Ideas with third parties for their marketing purposes** (emphasis theirs)."

They say the don't collect PII from children under 13 and ask that if you are under 13 you don't share any PII. They state they use SSL on "some" web pages were PII is collected. They remind readers that what they share are social media is outside of Freegal's control. They will retain PII "for the period necessary to fulfill the purposes outlined in this Privacy Policy or as required by law." The will share PII with "service providers," "business partners," and "DRM platform providers" for DRM authentication, lawyers and governments to comply with warrants and subpoenas, or to the relevant third party if Library Ideas (Freegal's parent company) is sold. They again assert, "Library Ideas does not sell or rent your personal information to third parties."

They do collect non-personal information and may, "use, transfer and disclose this type of non-personal information for any purpose." If they pair non-PII with PII it will be treated as PII . They use browser cookies which collect, "language, browser type, Internet service provider, referring and exit pages, clickstream data, operating system, Internet Protocol addresses, dates and times." which they do not consider PII.

In compliance with GDPR, the proactively state you can “access” the info they have about you and have it deleted. I tried emailing them to do this but email listed bounced back. They also listed a snail mail address to request such info. My letter to access my data and then have it deleted is in the mail.

Privacy Badger listed no trackers.

With all other add-ons turned off, Lightbeam shows my browser touching fourteen other sites besides my library’s website and Freegal’s website.

Does work on Tor? Yes. You can download songs and streaming player works too.

Overdrive

https://company.cdn.overdrive.com/policies/privacy-policy.htm?

The privacy policy is linked at the very bottom of the page in tiny print. They have a separate policy for children which is linked to from within master privacy policy. They recommend children read it with their parents and/or legal guardians.

They then define PII and non-PII. They do not collect PII unless patron chooses to submit it; e.g., you can create an “Overdive account” with your email but this is not required to use the service. Your email would be PII. If you submit PII, it will be protected via “secure sockets layer (SSL) technology” during transmission, and when at rest “firewalls and data encryption and physical access controls to our buildings and files.”

They do collect non-PII not limited to, “IP address, device type, device ID, operating system, library card number, Adobe ID, library name, digital content selections (e.g. lending history), and online activity.” You can share your lending history via their apps if you choose, otherwise it is “confidential” and only shared with library staff when necessary to fulfill duties or other as required by law. They use the info they collect to personalize the service (there is a long list of how they do this) and to “comply with the requirements of our publisher, library, and retail partners.“

They assert they will never sell your PII or non-PII, but they will share non-PII with third parties to improve their services. The may also “anonymize” PII in aggregate and share that with third parties for similar services. They will retain info “for as long as OverDrive deems necessary to provide the Services or as otherwise permitted by applicable law.”

There is a long section about how they use Cognito verification service for their online sign up option that some library’s use. Overdrive asserts Cognito will never share,

sell, or use for marketing purposes your PII. For brevity, I am not going to analyze Cognito's privacy policy. Overdrive notes that to use online sign up service they must gather significant PII. The assert they will never share or sell this info, but if you opt-in your info maybe used for marketing communications from Overdrive. They use three types of cookies: Required, Performance and Reliability, and Research and Analytics. You can opt-out the last two types, but the first is, um, required for Overdrive to work. They list the third party cookies they use: New Relic, Fabric, Google Analytics, and Google Adwords.

Much like the Children's privacy policy, their policy regarding cookies a separate document linked from the master policy. They use three types of cookies: Required, Performance and Reliability, and Research and Analytics. You can opt-out the last two types, but the first is, um, required for Overdrive to work. They repeat the third party cookies they use: New Relic, Fabric, Google Analytics, and Google Adwords. They mention you can opt-out of Google's cookies but don't provides instructions or links to where to do so. It is not mentioned in this document but there is a link at the bottom of Overdrive's labeled "Cookies settings." If you click it a window pops up that lets you toggle and off "Performance and Reliability" and "Research and Analytics" cookies.

Again, their GDPR compliance is separate document linked from the master document. It limits the request for access and deletion of personal data to EU residents only.

With all types of cookies turned on, Privacy Badger indicated one possible tracker for "google.com" but only the authentication page.

Will all types of cookies turned on and all other browser add-ons turned off, Lightbeam shows my browser touching twelve other sites besides my library's website and Overdrive's website.

Does it work in Tor? Ebooks—Yes. Audiobooks—No.

Lynda.com
https://www.lynda.com/aboutus/otl-privacy.aspx

At the very top, the name of the company and it's contact info, and in bold that you have a problem with the privacy policy don't use the service. It defines terms then again in all caps, "IF YOU DO NOT AGREE TO THIS PRIVACY POLICY, PLEASE DO NOT ACCESS OR USE OUR SERVICES."

They talk about which PII and non-PII they collect. More PII than a library services as Lynda.com is available for anyone who wants to pay. They say take "reasonable steps" to secure your data but don't get specific.

The list all ways they use your data and it is all personalization, credit cards, and then, "In any other way we may describe when you provide the information or when we prompt you regarding a new use of information about you."

They are only going to share your data unless required by law and "to a third party with your prior consent to do so." They reserve the right to transfer your data if they merge with another company.

They offer the user the ability to delete, amend, restrict (if they are doing something unlawful), or access they data they about you via their Customer Support, snail mail, or interestingly enough your "My Profile". They emphasize this data will be machine readable. I take this to mean not human readable. Later is says, "we will consider your request in accordance with applicable laws." If you cancel your account they will keep your info for a "reasonable amount of time." Even if you cancel your account they will keep your non-PII indefinitely.

Like Overdrive, they an entire separate cookies policy linked to repeatedly in the master privacy policy. By using the services you are agreeing to the use of cookies or "similar technologies." They define browser cookies, clear gifs, and (Adobe) Flash cookies. They say the these cookies will also be used on non-Lynda.com sites that host Lynda.com content. After defining yet more cookies, they say they use two types: persistent and session. Besides the personalization features, they state that cookies will be used for ads on and off Lynda.com. The explicit state that they ignore "Do Not Track" browser signals. They go on say they use "beacons, pixels, and tags." They explicitly say some ads will set third party cookies that will identify you, your browsing habits, and other info like IP address. They explicitly state the cookies will continue to do this even after you log out. The give link to a list of services they to do this with the caveat that the service providers could change.

They don't into specifics about the security, but mention they can't make it 100% secure and will let you know via email if there is a data breach.

There's a section about the "App" which collects of ton of stuff but the say they do not pair with your PII.

They say they never sell your PII to direct marketers without your permission.

With all other browser add-ons turned off, Lightbeam shows my browser touching nine other sites besides my library's website and Lynda's website.

Privacy Badger indicated one possible tracker for “google.com” when you actually started to watch a video on the site.

Does it work in Tor? No. You can log and navigate the site but videos won’t play.

Takeaways

Unsurprisingly, Freegal and Overdrive had more to say about keeping people anonymous and not sharing reading histories. Lynda.com openly says they are going to track you even when you are logged off. This is unsurprising given libraries’ value of privacy. All three though give themselves outs; e.g., they will never sell your info but they reserve the right to whatever they want with non-PII which we know can be reverse engineered. Being magnanimous, their legal departments are covering them for unforeseen circumstances. Being cynical, they are leaving room for them to do whatever they want. The deeper you go into each policy, the more caveats you find. Lynda.com’s was particularly bad. Their cookies policy was separate and it was there were their tracking policies really were. Freegal and Overdrive had shorter policies and the library friendly privacy assertions were near the top but the near bottom were legal caveats.

All reserved the right to keep your data indefinitely.

All said they took measures to secure user data but gave no specifics besides SSL.

I would describe Freegal and Overdrive’s as better but still problematic. I was left asking myself what an ideal privacy policy look like. Here’s a first shot:

- only collects PII when necessary
- collects non-PII only for service improvements
- any unnecessary collection is opt-n
- no third party cookies
- cookies don’t interfere with functionality
- a set time frame keeping data
- describe the security take to protect data
- make GDPR-like user requests easier. This might seem like a lot of work, but you can’t provide what you don’t have. If you designed your collection policies around requirements like this might make for less work in the long term.

If Lightbeam was correct, Freegal links to more sites, but works the best on Tor.