

Open letter to the Toronto Public Library about Hoopla and privacy

William Denton

May 8, 2014

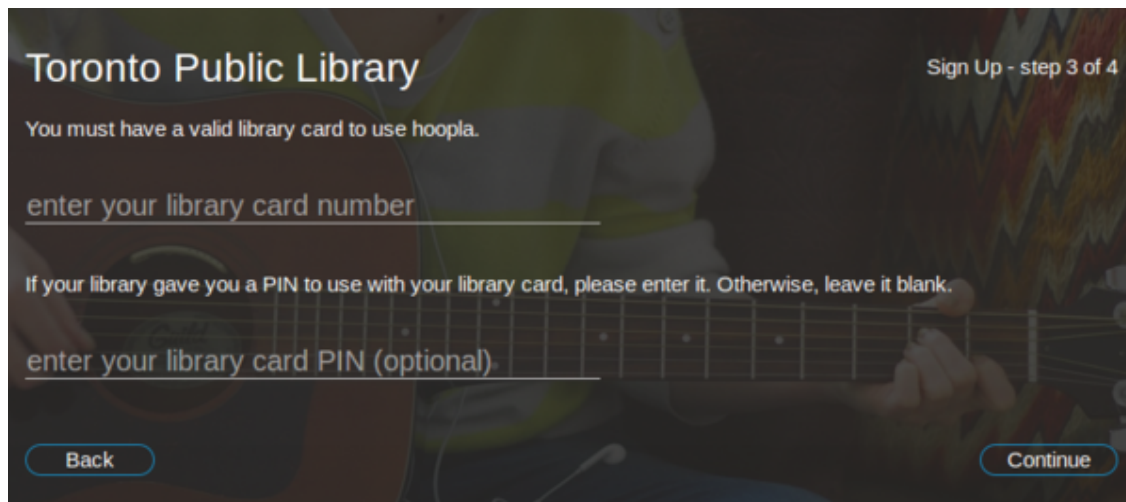
Jane Pyper (City Librarian, Toronto Public Library)
Michael Foderick (Chair, Toronto Public Library Board)

Toronto Public Library
789 Yonge Street
Toronto ON M4W 2G8

Dear Ms Pyper and Mr Foderick:

I am concerned about privacy issues with Hoopla, which the Toronto Public Library announced on Monday 7 April 2014 as “a new service that allows customers to download or stream a wide variety of music and video content.”¹

To use Hoopla, TPL users must create an account on its system. This is the third step in that process:



It is asking for the user's library card number and PIN. Everywhere else these are called the *username* and *password*, so let's use those terms. Using Hoopla requires that the user tell it their Toronto Public Library username and password. I strongly object to this. It is wrong and it is unnecessary.

TPL should never ask users to give away their usernames and passwords. Online security is difficult and complex in many ways, but a fundamental rule is that *you never ever give away your username and password*, especially for

¹http://torontopubliclibrary.typepad.com/news_releases/2014/04/toronto-public-library-introduces-online-music-and-video-.html

something as private and personal as your library account. Educating users about online security is an important job for libraries today, and part of that is embodying and encouraging best practices. TPL should be *helping* its users to never give away their usernames and passwords, but instead, it is actively *encouraging* them to do just that. The only mention of privacy is a mild suggestion that users “may wish to review [Hoopla’s] privacy policy,”² with no mention that the company is in the United States. Because Hoopla is American, these usernames and passwords are available to the US government through the PATRIOT Act. It is a fundamental duty of libraries to protect their users’ personal information. I believe TPL generally does a good job of that but here it has abandoned its role.

TPL’s privacy policy³ permits the Hoopla service. Section A.4 says, “The Library will not disclose personal information related to a visitor or library user to any third party without obtaining consent to do so, subject to certain exemptions as provided in section 32 of MFIPPA.” Specific directive 4 says, “Third party service providers will be required to ensure, by means of a statement in their contract, that any staff or users’ personal information to which they have access is only to be utilised for the purposes of carrying out the service they provide to the Library and for no other purpose.” The fact that TPL’s privacy policy allows it to encourage users to give away their usernames and passwords to an American company, with only the feeble assurance of “a statement in their contract,” does not justify or validate the Hoopla offering. It means the privacy policy is broken.

Hoopla’s privacy policy⁴ is brief and clear but it does not ensure complete privacy. It says, “We use your library card number and library card PIN to authenticate you with your library’s systems” and “All electronic communication between your web browser or mobile device and our servers is protected and encrypted via SSL (HTTPS). Your password is encrypted before it is stored in our database.” Sadly, any mention like that of encryption is essentially meaningless: there are many bad ways to encrypt passwords in databases. As well, there is no mention of how the communication between Hoopla and TPL is done and if that is secure. Hoopla also says, “We use a record of the materials you borrow to bill your library for usage, and to pay content providers a fee for distributing the content they have licensed to us.” Hoopla does not say it deletes old borrowing records (as TPL does) so we must assume all borrowing is stored permanently on its servers. Hoopla says, “We may also release your information when we believe release is appropriate to comply with the law, enforce our site policies, or protect ours or others rights, property, or safety.” That is not reassuring. Finally, there is no clear mention that Hoopla is in the United States and subject to the provisions of the PATRIOT Act and other American legislation. In my opinion Hoopla’s privacy policy does not meet the standards that should be required by third-party providers used by the Toronto Public Library. Again, the fact that it does means TPL’s privacy policy is broken.

Beyond all those policy problems, there is no reason why TPL need require its users to give their usernames and passwords to Hoopla. It is perfectly possible for Hoopla to ensure someone is a valid TPL user without ever knowing their username and password, just as how people can log in to web sites using their Facebook or Twitter account. If I log in to web site X using my Twitter credentials, the site passes me over to Twitter, which asks me, “Would you like to share your name and email address with X?” If I agree, Twitter passes me back to X, which now knows my name and email address and that I am a valid Twitter user—but *X never asked me for my Twitter username and password.*⁵ If Hoopla and TPL can’t do that, it means their systems are inadequate. This needs to be fixed before insecure new services are offered.

There are problems with every level of the Hoopla offering. They would all be met by following the basic principles of the “Privacy by Design” guidelines⁶ set out by Dr. Ann Cavoukian, the Information and Privacy Commissioner of Ontario:

1. Proactive not reactive; preventative not remedial

²<http://www.tpl.ca/hoopla>

³<http://www.torontopubliclibrary.ca/terms-of-use/library-policies/access-to-information-protection-privacy-policy.jsp> (last revised 21 June 2010)

⁴<https://www.hoopladigital.com/privacy> (last revised 5 February 2013)

⁵This is done with OAuth (<http://oauth.net/>), which says on its web site, “If you’re storing protected data on your users’ behalf, they shouldn’t be spreading their passwords around the web to get access to it. Use OAuth to give your users access to their data while protecting their account credentials.”

⁶<http://www.ipc.on.ca/english/Privacy/Introduction-to-PbD/>

2. Privacy as the default setting
3. Privacy embedded into design
4. Full functionality — positive-sum, not zero-sum
5. End-to-end security — full lifecycle protection
6. Visibility and transparency — keep it open
7. Respect for user privacy — keep it user-centric

I encourage TPL to consult with the IPC and security experts. I request the Toronto Public Library to revisit and enhance its privacy policy and to improve its information technology services so that fully private and secure third-party services can be offered.

Yours sincerely,

William Denton <w Denton@yorku.ca>
Web Librarian, York University Libraries
102N Steacie
York University
4700 Keele Street
Toronto ON M3J 1P3

cc:

- Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario