Web Privacy in Practice: Assessing Internet Security and Patron Privacy in North American Public Libraries

Abstract:

There are a variety of software solutions that libraries may offer users of public internet terminals (PITs) in order to protect their privacy and enhance security. To determine the rate of adoption and support for these technologies, an online survey was sent to 176 urban and suburban public library systems in the United States and Canada. Questions pertained to:

- default use of private browsing on PITs,
- implementation of anti-tracking and security-enhancing browser add-ons
- education on or use of Tor, an anonymizing network

Separately, the authors conducted an audit examining the default use of HTTPS for library websites and catalogs.

The majority of responding libraries are not making use of any privacy- or security-enhancing browser add-ons. Nor are they promoting the use of Tor. Similarly, education programming about privacy and security is relatively uncommon.

While the majority of libraries sampled are not using HTTPS, it is more common to use HTTPS to encrypt online catalog queries than basic library webpages. Library support for secure, private — and, if necessary, anonymous — communications on public access computers remains minimal.

Introduction:

What security measures are used on library PITs? Many best practices exist — including routine plugin updates, defaulting to private browsing and/or clearing web cache between sessions (Phetteplace, 2012), and making use of privacy-enhancing browser extensions such as HTTPS Everywhere — to protect patrons from unwanted data disclosure as well as surreptitious tracking of web browsing behavior (Henry, 2015; Anonymous, 2015).

Melissa Morrone (2014) has written that libraries could easily empower their users with encryption and anti-tracking software. Recently, some libraries have expressed interest in giving their patrons access to anonymizing tools such as Tor (Koebler, 2015; Warburton, 2015). How many libraries actually follow these practices, however?

Presented below are the results of a survey of public libraries designed to assess the security and privacy software being offered to patrons using PITs as well as efforts to educate patrons regarding these tools.

Methods:

PARTICIPANTS:

176 libraries in North America were selected for this study; 45 from Canada and 131 from the United States. The criterion for inclusion was institutional membership in either the Canadian Urban Libraries Council (CULC) or the Urban Libraries Council (ULC); these organizations count among their members the largest library systems serving urban and suburban communities in their respective countries.

MATERIALS:

The survey instrument included 10 primary questions, divided into 3 sections — all questions pertained to software available on public computers and the configuration thereof. The survey branched to include 4 follow-up questions depending upon previous answers.

- Section 1 (three questions) pertained to support for private browsing and default web search configurations.
- Section 2 (four to seven questions) pertained to use of privacy- and security-enhancing browser add-ons.
- Section 3 (three to four questions) pertained to support for and education about Tor.
- An audit of the use of HTTPS to serve general library and library catalog pages was also conducted.

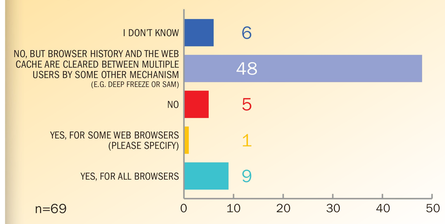
PROCEDURE:

The Qualtrics survey was distributed in a link via email. Responses of individual staff members who were clearly listed on library webpages as having oversight for information technology were solicited where that information was publicly available; when no such individual was identifiable, or their contact information was not public, a response was solicited from a library's publicly disclosed "information" or "administration" email address.

All responses were anonymous; no analytics were used to collect institutionally identifiable information such as IP addresses. In order to differentiate responses from the separate countries, identical surveys with separate links were sent to libraries based on their CULC or ULC membership.

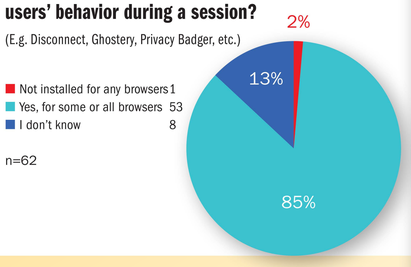
The HTTPS audit was conducted using Internet Explorer 10; it involved manually visiting all CULC and ULC library homepages to record whether they enforced HTTPS connections by default. The process was repeated for the landing page of each library's public access catalogue.

Is private browsing (a.k.a. "Incognito Mode" or "InPrivate Browsing") the default setting for cookies and the web cache on public access computers at your library?

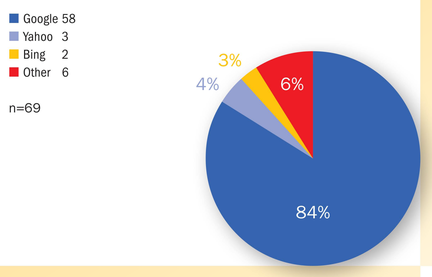


Do any of the browsers on your library's public access computers have extensions that stop advertisers or other third-parties from tracking users' behavior during a session?

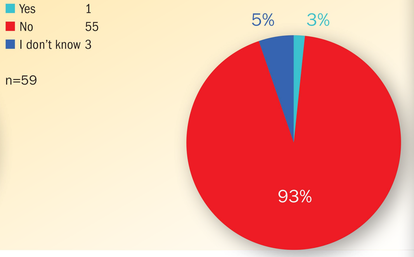
(E.g. Disconnect, Ghostery, Privacy Badger, etc.)



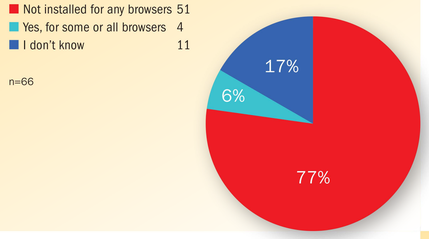
What is the default web search engine on public access computers?



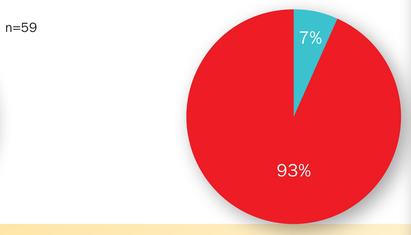
Does your library run a Tor (The Onion Router) Relay or Bridge?



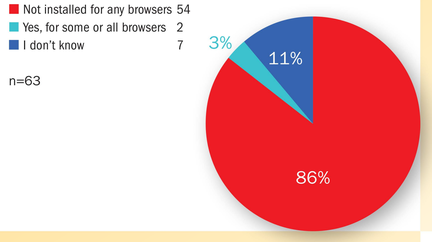
Is the HTTPS Everywhere browser extension installed and configured on public access computers in your library?



Is Tor made available on public access computers?

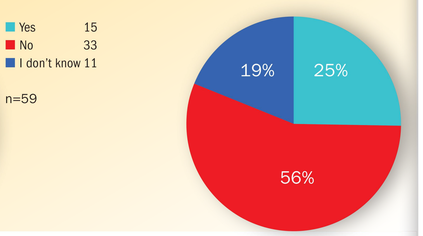


Is the WOT (Web of Trust) browser extension installed and configured on public access computers in your library?

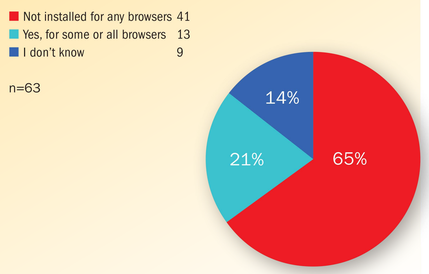


Has your library ever offered any type of instruction to patrons about online anonymity and/or privacy?

Possible subjects might include Tor, Virtual Private Networking, HTTPS, browser extensions for home computing, or similar.

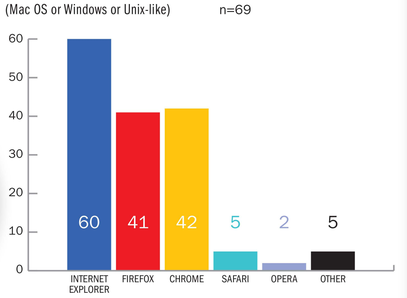


Are any ad-blocking browser extensions (e.g. Adblock, Adblock Plus) available on public access computers in your library?



What web browsers are available on public access computers at your library?

(Mac OS or Windows or Unix-like) n=69



Results:

Of the 176 libraries in the sample, 69 responded to the survey for a response rate of 39%. This rate is low, yet still allows generalization to the entire sample of CULC and ULC member libraries with a 95% confidence level at a 10% margin of error. Libraries from CULC accounted for 28 (41%) of respondents; ULC libraries accounted for 41 (59%) of respondents. No anomalous differences were observed between libraries located in Canada and those in the United States. All questions were optional; so, while 69 libraries completed most of the survey, some questions were skipped and have lower response rates. The number of respondents (n) is displayed for each question. For the HTTPS audit, all 176 libraries were examined.

- Section 1: Default Web Browser & Web Search Configuration
- Section 2: Privacy & Security-Enhancing Add-Ons
- Section 3: Anonymizing Network Support
- HTTPS Audit

Discussion/Conclusion:

Limitations: The survey's anonymous design precludes any follow-ups or attempts to track individual institutional change longitudinally. It also inhibits correlating survey responses with the results of the HTTPS audit, thereby preventing any ranking of institutions on their privacy and security efforts. The invitation to self-report introduces the question of cognitive bias around social desirability, but this may be mitigated to some extent by the anonymity of the response platform.

Secure Browsing using HTTPS: The use of TLS/SSL to transmit HTTP protocol communications (HTTPS) encrypts them, to a certain degree, and ensures data integrity. It might be expected that libraries, which justifiably protect patron checkout records in accordance with our established professional ethics, would apply similar privacy principles to the online environment.

Without the use of HTTPS on library websites and online catalogs, patron queries and behavior are highly susceptible to eavesdropping and forgery ("spoofing" attacks) (Macrina, 2015). No library would tolerate non-library staff physically observing and recording patrons' catalog usage or attempts to impersonate library staff; they should not tolerate online equivalents of these behaviors either.

Promisingly, the American Library Association (ALA) is a financial sponsor of the Let's Encrypt initiative to deploy TLS/SSL for the internet at large, but our results indicate that many libraries are not yet living up to ALA's rhetoric around electronic privacy.

PRIVACY AND ANTI-ADVERTISING SOFTWARE ON PUBLIC COMPUTERS:

As libraries protect users' privacy in their physical spaces, most also frown on the use of library space and resources as advertising platforms except in limited and targeted instances (sponsorship of facilities, for example) — we would expect this to hold especially true if prospective advertisers were demanding personally identifiable information about library users' habits and inclinations.

The open internet is rife with obtrusive advertising and heavily underlaid with analytics and advertising trackers of every description which collect, collate, and often sell information about the habits of website and social media users. Often, such trackers operate longitudinally, following a user from website to website to build more comprehensive data about browsing and use habits (Madrigal, 2012). As cryptography and privacy expert Bruce Schneier (2014) has noted: "Surveillance is the business model of the Internet."

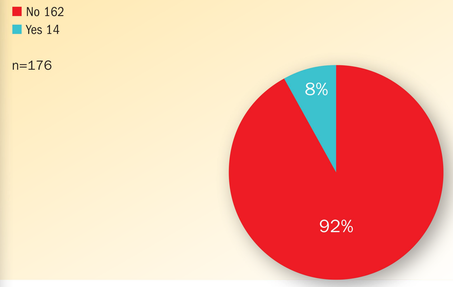
Many tools — such as Ghostery, Disconnect, and Privacy Badger — aim to mitigate this state of affairs by disallowing specific trackers; 85% of responding libraries deploy some anti-tracking add-on in some browsers, a promising sign. However, a follow-up question with a low response rate (n=12, results not depicted due to space considerations) revealed that Firefox is the primary browser equipped with these software options. Users of other browsers are typically left defenseless. Anti-advertising tools are clearly underused; 65% of respondents admitted that ad-blocking add-ons are not deployed to any browsers. Some patrons may want to view web advertisements and should be given that option; likewise, libraries should give patrons the ability to opt-out of the advertising-industrial complex if they so choose. Our results show that libraries can do a better job protecting users from unsolicited, intrusive, and possibly malicious advertising and analytics.

ANONYMITY NETWORKS:

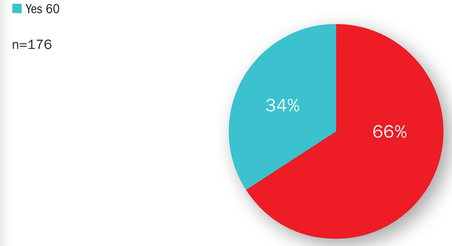
Onion routing networks, of which Tor is by far the best-known and most widely-used example, represent the current gold standard for online anonymity. Tor recently made headlines in the library world when a public library in New Hampshire was subjected to intimidation from law enforcement and the Department of Homeland Security because it was running a Tor relay (Brooks, 2015). In spite of this high-profile case, only one responding library indicated that it was running a Tor relay; fewer than 10% of respondents facilitated access to Tor in any way at all.

Even more surprising, over half of respondent libraries indicated that they had never offered any educational programming whatsoever regarding online anonymity and/or privacy; only 25% of respondents could conclusively say they had ever offered any such programming. These results indicate that libraries have a considerable way to go in educating and facilitating online anonymity – and indeed basic data security – for their users.

Are Library Pages Served HTTPS by Default?



Are OPAC Pages Served HTTPS by Default?



REFERENCES:

Anonymous. (2015). *Library privacy audit.* Unpublished collaborative manuscript. Retrieved from https://www.piratepad.ca/p/Library_Privacy_Audit

Brooks, D. (2015, September 11). Lebanon library at center of internet privacy debate in shutting off its Tor server. *Concord Monitor.* Concord, NH. Retrieved from http://www.concordmonitor.com/readerservices/businessxml/18550899-95/lebanon-library-at-center-of-internet-privacy-debate-in-shutting-its-tor-server

Henry, A. (2015, August 31). The best browser extensions that protect your privacy. *Lifehacker.* Retrieved from http://lifehacker.com/the-best-browser-extensions-that-protect-your-privacy-479408034

Koebler, J. (2015, September 17). A dozen libraries want to host Tor nodes to protest government fearmongering. *Vice | Motherboard.* Retrieved from http://motherboard.vice.com/read/a-dozen-libraries-want-to-host-tor-nodes-to-protest-government-fearmongering

Macrina, A. (2015, January 27). Why we need to encrypt the whole web... library websites, too. *LITA Blog.* Retrieved from http://litablog.org/2015/01/why-we-need-to-encrypt-the-whole-web-library-websites-too/

Madrigal, A. C. (2012, February 29). I'm being followed: How Google—and 104 other companies—are tracking me on the web. *The Atlantic.* Retrieved from http://www.theatlantic.com/technology/archive/2012/02/im-being-followed-how-google-151-and-104-other-companies-151-are-tracking-me-on-the-web/253758/

Morrone, M. (2014, July 8). How your library can help you resist the surveillance state. *Waging Nonviolence.* Retrieved from http://wagingnonviolence.org/feature/local-library-can-help-resist-surveillance-state/

Phetteplace, E. (2012). Hardening the browser: Protecting patron privacy on the Internet. *Reference & User Services Quarterly, 51*(3), 210-214.

Schneier, B. (2014). *Bruce Schneier talk at MIT.* Cambridge, MA. Retrieved from https://d1baxxa0joomi3.cloudfront.net/20010d06fe480b67ae457c7e947b2caf/basic.mp4

Warburton, B. (2015, September 21). New Hampshire library reaffirms Tor Project participation. *Library Journal.* Retrieved from http://lj.libraryjournal.com/2015/09/digital-resources/new-hampshire-library-reaffirms-tor-project-participation/

ACKNOWLEDGEMENTS:

We would like to thank the following individuals for their assistance and advice on data collection:

Galen Charlton, *Equinox Software, Inc.*

Katherine Bates, *Urban Libraries Council*

This project would not have been possible without the support and guidance of **Alison Macrina** and the **Library Freedom Project.**

OUR CONTACT INFORMATION:

Gabriel Gardner
Reference & Instruction Librarian, CSU Long Beach
gabriel.gardner@csulb.edu

Myron Groover
Archives & Rare Books Librarian, McMaster University
groover@mcmaster.ca