Minitex

REFERENCE NOTES

August 2013

Simple Tools to Refract PRISM in Your Library

Gabriel J. Gardner, Reference Librarian, University of Minnesota, Duluth

Spurred by recent revelations about the breadth of the National Security Agency's data-gathering practices, ALA is encouraging members to host or moderate public forums on the issue. In an open letter to American Library Association members on July 11th, ALA President Barbara Stripling urged libraries to facilitate public dialogues to educate Americans about their First and Fourth Amendment rights. Regardless of how they might feel about the legality or morality of Mr. Snowden's actions, librarians across the nation owe him a debt for teaching the general public the word "metadata." For many Americans, the news coverage and public discourse surrounding PRISM and Upstream has enriched their understanding of data-about-data in a way that no library publicity or programming could. Fortunately, there are a number of free software and service options that libraries can provide for their patrons to help them use the Internet in a more secure and private fashion.

Much of the software recommended below is open-source and deliberately recommended because of that. Closed-source alternatives exist for many of these options but should be viewed with a skeptical eye. According to The *Guardian*, Microsoft's Skype includes a 'backdoor' that allows NSA and FBI analysts to surreptitiously monitor encrypted conversations in addition to collecting metadata. Additional 'backdoors' to Google, Apple, and Dropbox are the subject of plausible speculation. Closed-source programs may also contain 'zero day' exploits – known bugs which allow third-parties to gain access to various tasks on the target computer(s). Open-source software is theoretically less susceptible to both backdoors and zero day exploits; with source code being scrutinized and maintained by various individuals, "given enough eyeballs, all bugs are shallow."

DuckDuckGo & Startpage
https://duckduckgo.com/
https://www.startpage.com/

Worried that Google or Microsoft keep your search history? Concerned about filter bubbles? Switch your search engine and rest easy. In the reaction to Mr. Snowden's leaks, two search engines have been gaining in popularity, DuckDuckGo and Startpage. Neither service saves searches nor shares them with your destination site. Neither service collects IP information for location tracking (this can of course lead to less relevant results). Since no searches or IP information are saved or associated, no filter bubbles are created; the same search string will produce the same results from any computer in the world. Startpage goes the extra mile and allows users to browse pages via a proxy server, extending the user's anonymity. Librarian pro-searchers will be happy to learn that both DuckDuckGo and Startpage support specific domain searches (query site:example.com). DuckDuckGo and Startpage can be set as the default search or added to the search box in Firefox, Chrome, Opera, and Internet Explorer.

Disconnect
https://disconnect.me/

The NSA isn't alone in tracking; marketers have been at it for years. With privacy now on more patrons' minds, it is a fine time to remind them of surveillance in the private sector. Every day, thousands of companies track web traffic and search strings using a variety of methods including cookies, IP addresses, and the complex method of 'browser fingerprinting.' Disconnect is a browser extension that blocks known advertising, analytics, and social media tracking attempts. Blocking tracking attempts doesn't just increase privacy, it decreases page load time; according to Disconnect, with their extension installed, pages load an average of 27% faster. Disconnect is available for Firefox, Chrome, and Safari.

HTTPS Everywhere
https://www.eff.org/https-everywhere

The web is open by design and HTTP connections are not encrypted. HTTPS Everywhere is a browser extension that rewrites communications between a browser and server to use HTTPS with supporting websites. HTTPS offers two-way encryption between browser and server, which prevents eavesdropping and forging of HTTP communications. With HTTPS Everywhere, users are far less likely to fall for spoofing attacks or to have their login information obtained by third parties. Many sites offer HTTPS but may not use it by default (Yahoo! Mail did not offer HTTPS at all until 2013), HTTPS Everywhere fixes this automatically behind the scenes, ensuring that if a website supports HTTPS, the browser will use it. HTTPS Everywhere is available for Firefox and Chrome.

Cryptocat
https://crypto.cat/

Internet chat is a longstanding and popular communication medium. Cryptocat is a browser extension that provides encrypted chat for private messaging or many users in a chat room. Many chat clients use and support Off-the-Record Messaging (OTR), which provides encryption for instant messages. Cryptocat takes OTR one step further by encrypting all communications on the client side; no unencrypted messages are transmitted. CryptoCat takes privacy seriously and saves no metadata of chats. Users should be aware that communications are not totally anonymized; for IP anonymity Cryptocat would need to be combined with Tor or a virtual private network, both of which are probably not suitable for use on public computers. Cryptocat is available for Firefox, Chrome, and Safari.

TrueCrypt
http://www.truecrypt.org

Some patrons will want to encrypt more than their chats and web traffic. TrueCrypt provides real-time, "on-the-fly," disk encryption in addition to other features. TrueCrypt creates encrypted virtual volumes or partitions in which users can store data they would like to keep secure. Administrator privileges are required to create volumes so TrueCrypt cannot safely be installed on public access computers. However, the application is of modest size and can run off most USB sticks with plenty of room left for the encrypted data. Once the virtual volumes are created on a portable USB drive, a user only needs to remember her password to work securely at any public computer. TrueCrypt is available for Windows 7/Vista/XP, Mac OS X, and Linux.

Take a real stand
Used individually, these tools offer marginal improvements in privacy, security, and anonymity. Deployed in concert, they offer significant protection. Installation of Disconnect, HTTPS Everywhere, and Cryptocat is as simple as adding any other browser extensions. Setting DuckDuckGo or Startpage as the default browser search requires several clicks but is no serious obstacle. Libraries seeking to heed Barbara Stripling's call and take a stand for privacy should seriously consider installing these tools on public computers and educating their patrons about their use. Facilitating public dialogue on privacy and surveillance is only a first step. Providing citizens with the means to protect privacy and resist surveillance is taking a stand. ■