The Tor Browser and Intellectual Freedom in the Digital Age

Alison Macrina

Alison Macrina *is a librarian, privacy activist, and the founder of the Library Freedom Project, an initiative which aims to make real the promise of intellectual freedom in libraries. She can be contacted via alison@libraryfreedomproject.org or libraryfreedomproject.org.*

Correspondence concerning this column should be addressed to ***Eric Phetteplace****, Systems Librarian, California College of the Arts, 5212 Broadway, Oakland, CA 94618; email: ephetteplace@cca.edu*

I have wanted to publish a column on privacy as it relates to library technology for a while. While privacy has always been an issue at the forefront of librarians' minds, revelations surrounding the NSA's far-reaching data-collection programs and a seemingly unending string of high-profile breaches at major companies make paying attention to privacy all the more pressing. Having discovered Alison Macrina's work via an appropriately-titled article "Radical Librarianship: How Ninja Librarians are Ensuring Patrons' Electronic Privacy," she was an obvious choice for author. Her work with the Library Freedom Project is vitally important to the future of libraries and recently earned a Knight Foundation grant.—*Editor*

If you've been following the revelations of the last year and half detailing the overbroad and often illegal collection of data by the NSA surveillance machine and its various government and corporate partners, you've no doubt heard of Tor. It's a powerful tool for anonymity, one of many tools that whistleblowers like Edward Snowden, activists, journalists, and everyday people use to help conceal their identities online. The Tor web browser was featured in some of NSA slides that Snowden leaked (see figure 1); according to the spies, it's a tool for terrorists and other criminals, which ignores the many legitimate reasons noncriminals might want to conceal their sensitive personal data from spies and hackers. Other Tor-haters insist, without evidence, that the browser is actually an NSA false flag, designed to trick users into thinking that it's protecting their online activity, but in fact designed to compromise privacy, or that it's been broken by cryptographers working for the government—or that it never even worked at all. Many false, sometimes deliberately misleading, things are written about Tor, and the people smearing it seem to want Tor banned or shut down outright (for a thorough explication and evisceration of some of the major condemnations of Tor, read this perfectly-worded blog post from *The Intercept*'s Micah Lee).[1] What is it about Tor that causes such controversy?

Tor is a powerful tool that gives users anonymity in an age of total online surveillance. It's misunderstood and therefore sensationalized by a nontechnical media and public. But it's also something that librarians need not only to understand, but to champion and fight for. Why? In this era of dragnet surveillance, our freedom to read and write freely is threatened. A recent PEN study entitled "Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor" detailed this well, showing that one in six writers polled had self-censored because of fears of surveillance, and another one in six had seriously considered doing so.[2] This is an

Figure 1. "Terrorist with Tor client installed" from one of the NSA slides revealed by Edward Snowden to Glenn Greenwald in June 2013.

alarming statistic, one that shows how much surveillance threatens free expression. There are few things librarians care more about than intellectual freedom, and Tor can help our local communities protect that freedom. This is why libraries should be installing the Tor Browser on all public PCs, running Tor relays from our networks, and teaching the public what Tor is and how they can use it to protect themselves.

To help our library community understand this tool, a little background on Tor and how it works is necessary. First, just what *is* Tor? The most simple definition comes directly from the folks at the Tor Project: "Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet."[3] The most common use of Tor is through its web browser, which you'll see referred to as "the Tor Browser," "the Tor Browser Bundle," or sometimes simply "Tor." Tor is fundamentally a proxy that masks the location information and browsing history of the user, allowing for anonymous use of the Internet. Tor can be used with email, instant messaging clients, cell phones, and more to route communications over the Tor anonymity network. Tor services are made possible by a network of relays that encrypt the original user's traffic so that the location information cannot be discovered. In this article, I'm mostly going to be discussing the Tor Browser and its potential uses in libraries. When referring to the Tor network as a whole, I'll call it simply "Tor." For more on Tor's history and other Tor services, be sure to visit https://www.torproject.org.

The Tor Browser was built from an "onion routing" project of the US Navy, which was designed to protect military communications, and was turned into an independent (non-military) project by developers Roger Dingledine and Nick Mathewson in 2002. Onion routing bounces traffic from the original user across a network of three relays, providing three layers of encryption (like the layers of an onion, hence "onion routing," and the Tor onion logo) and masking the original IP address from the user's computer. Today, it's used by about four million people worldwide to evade censorship and surveillance, allowing users to access blocked websites in Internet-restrictive countries like Iran and China (because typically websites rely on IP location information to restrict access), keeping journalistic sources safe, and masking the identity of whistleblowers. Reporters Without Borders recommends that journalists reporting from dangerous places use Tor to protect themselves.[4] Tor features prominently in the Electronic Frontier Foundation's "Surveillance Self-Defense" playlists for safer online communications.[5] One of my personal favorite use cases for Tor is combatting digital stalking of domestic violence victims by their abusers.[6] Often those abusers will obsessively stalk their victim's online accounts, trying to find out where he or she might be living, or use tools to compromise victim's cell phones and determine real-time location information. Members of the Tor Project have installed the Tor Browser (along with other anonymity tools) onto the computers in domestic violence shelters to help protect these users, as well as protect the location of the shelters themselves. Online anonymity should not be dismissed as something desired only by those with something criminal or nefarious to hide, but as a vital tool for human rights, speech, privacy, security, and intellectual freedom. Cue libraries.

Patrons already seek us out to teach them how to use technical tools, and we've been staunch defenders of intellectual freedom and privacy from our earliest days. Libraries serve many people from marginalized communities, including immigrants, Muslim-Americans, people of color, people who are or have been homeless or incarcerated—and marginalized people are under even more surveillance than the general public. As a way of continuing our professional commitment to intellectual freedom and social justice values, installing the Tor Browser on our public computers and teaching it to our patrons in computer classes is an obvious choice.

Using the Tor Browser is a bit different than the browser experience most of our patrons are familiar with, but by following the Tor Project's best practices and establishing some of our own, we can help our patrons get the most out of this powerful privacy tool.

The first step is downloading the Tor Browser from https://www.torproject.org and checking the PGP (pretty good privacy) signature to make sure that the version you're downloading is the real Tor Browser and not a fake version created by an adversary. That's right, there are indeed bad people out there who want to tamper with the Tor Browser, so signature verification is an important step to ensure the integrity of the software.[7]

The first time you open the Tor Browser, you'll get a prompt to "connect or configure" (see figure 2). Most users, particularly those in libraries, will only need to connect directly, but I encourage you to click through the configuration

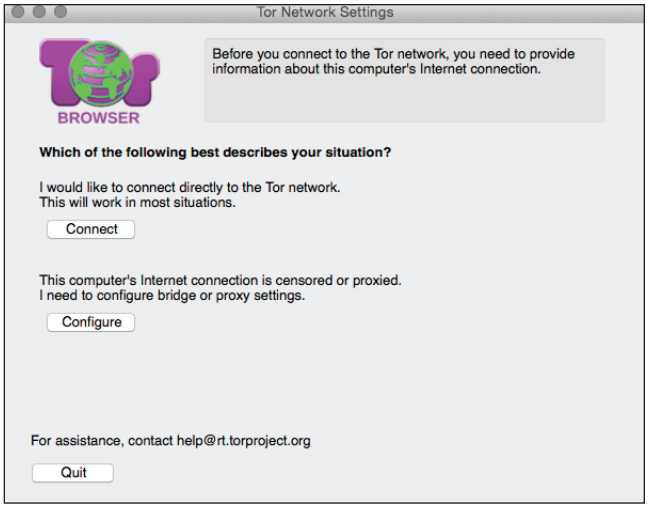

Figure 2. The "connect or configure" window you'll see the first time you open the Tor Browser.

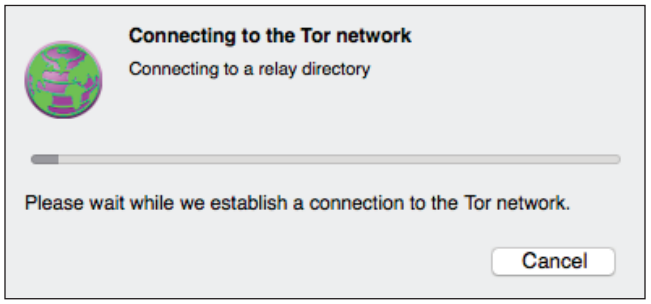

Figure 3. Connecting to the Tor Network.

prompts so you can get a sense of how the Tor Browser can be used in proxied or censored networks.

Once you click "connect," you'll see a second window establishing a connection to the Tor network (see figure 3). This window will appear every time the Tor Browser is opened. Sometimes the connection can take a few moments to establish—the Tor network can be pretty slow at times. That's because the network relies on volunteer-run relays all over the world to help keep its traffic moving. If more people or institutions ran Tor relays, the network would be much faster—more on that later.

After you've successfully connected, your browser will open with the message seen in figure 4: "Congratulations, your browser is configured to use Tor!" Now, take a moment to look around. You'll notice the default search engine is Startpage, which is an anonymous search engine that doesn't track you. The Tor Browser also comes with two extensions installed: HTTPS Everywhere and NoScript. HTTPS Everywhere is an awesome tool from the Electronic Frontier Foundation that forces compatible websites to use HTTPS by default for added browsing security.[8] NoScript (https://noscript.net) is an extension that blocks Javascript, Java, and Flash, because these scripts can deanonymize Tor Browser users. It's not

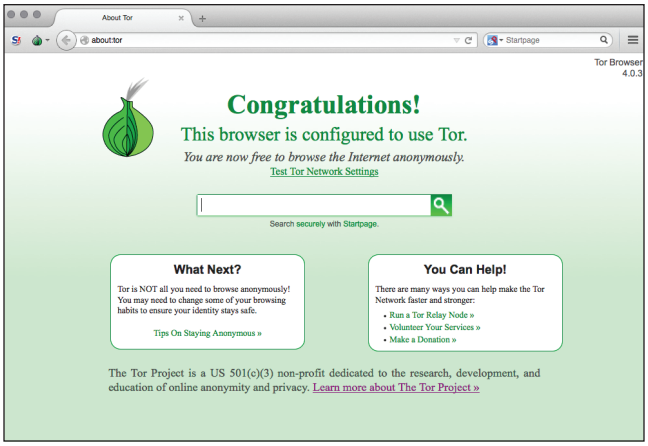

Figure 4. The Tor Browser when opened. Notice the Startpage search engine (in the center of the screen and on the top right as a search bar), as well as the NoScript extension (top left) and Tor Button (top left). The HTTPS Everywhere extension is not displayed, but it's installed.

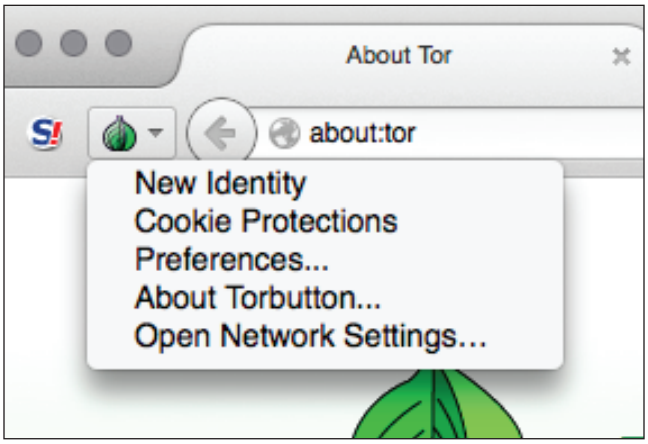

Figure 5. The Tor Button with its menu open.

recommended to add any more extensions to the Tor Browser because other extensions could compromise the user's anonymity as well.

Another thing you'll see on the Tor Browser is the Tor Button (see figure 5). This cute little onion allows more advanced users to make changes to Tor Browser settings and preferences, and you can also easily request a "new identity"—that is, a new IP address from the one the Tor Browser has assigned. You can view the IP that the Tor Browser has assigned you by clicking "Test Tor Network Settings" on the Tor Browser homepage. The IP you've been assigned corresponds to the relay your traffic has exited from, and you can view this information in the Tor Network Settings too. Sometimes it'll be an actual location, and sometimes it'll say "anonymous proxy." Keep in mind that whatever IP you've been assigned will affect your browsing experience! So if your assigned IP address is in Germany, some sites, like YouTube for example, will appear in German.

There are important best practices and some limitations to keep in mind when using the Tor Browser. Users should avoid accessing identifying accounts, like Facebook and email, through Tor, unless they actually create the account using the Tor Browser. Otherwise, the account can be linked back to whatever non-Tor browser they've used in the past, compromising their location anonymity. Users should only download through the Tor Browser if they trust the site they are downloading from—otherwise, they can be easily deanonymized. Torrenting should be completely avoided in the Tor Browser—the Tor network can't handle the load, and it will make things slow for other Tor users. Websites that require scripts to function properly won't work well with the NoScript extension default settings (all scripts blocked), but users can enable scripts for trusted sites.[9] Some sites will require Tor Browser users to complete additional security checks, usually CAPTCHAs. It's also important to remember that the Tor Browser is not a salve for total anonymity—users should understand the risks, and depending on what their personal needs are, they may want to take additional measures to keep their digital communications safe. For more on extra privacy-protecting steps and best practices, visit the Tor Project's website (https://www.torproject.org).

Relays are the backbone of the Tor network, passing traffic between each other to make the three layers of anonymizing encryption possible. A relay requires one computer and at least 250 kbps of bandwidth in each direction. You can run a Tor relay on any operating system. Downloads and instructions for running a relay can be found at https://www.torproject.org/docs/tor-doc-relay.html.en. Make sure to read all the instructions in full before starting the installation. Once your relay is set up, you don't have to do anything else—it'll just run quietly on your network. You can even view how much traffic is coming and going from your relay by looking it up on the Tor atlas.[10] Don't worry—you won't be able to see any of the identifying information of the original user (that would defeat the whole purpose of Tor). The atlas just shows the volume of traffic.

Libraries should be installing the Tor Browser on all of our public computers as well as teaching it in computer classes and one-on-one tech sessions with patrons. We can encourage the use of the Tor Browser by training our staff to field questions about this browser and staying up to date on efforts by the Tor Project to make the Tor Browser even more powerful and usable. We should make signs and place them around our computer areas, introducing users to the Tor Browser and explaining in brief some of its best practices for use. Even if our patrons only open the Tor Browser and leave it running in the background while they surf the web from another browser, that still strengthens the anonymity of the network as a whole—more users means more protection for everyone. For assistance installing and using the Tor Browser in libraries, including training materials for staff and public users alike, you can visit my website (library freedomproject.org).

As librarians, we affirm our commitment to intellectual freedom by celebrating books that have been banned or challenged, rejecting censorship of our collections and our computers, and upholding privacy as one of our professional core values. Using and teaching the Tor Browser is just another way we can celebrate our commitment to the democratic values of free expression and free speech.

Notes

1. Micah Lee. "Fact-Checking Pando's Smears Against Tor," *Micah Lee's Blog*, December 11, 2014, https://micahflee.com/2014/12/fact-checking-pandos-smears-against-tor.
2. PEN America, "Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor" (New York: PEN American Center, 2013), www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf.
3. "Tor: Overview," Tor Project, accessed February 15, 2015, https://www.torproject.org/about/overview.
4. Reporters Without Borders, accessed February 15, 2015, https://en.rsf.org/reporters-without-borders-and-25-04-2014,46196.html.
5. Electronic Frontier Foundation, "Surveillance Self-Defense: Tips, Tools and How-tos for Safer Online Communications," accessed February 15, 2015, https://ssd.eff.org.
6. Cory Doctorow. "Tor: Network Security for Domestic Abuse Survivors," Boing Boing, May 7, 2014, http://boingboing.net/2014/05/07/tor-network-security-for-dome.html.
7. Tor Project, "How to Verify Signatures for Packages," accessed February 15, 2015, https://www.torproject.org/docs/verifying-signatures.html.
8. "HTTPS Everywhere," Electronic Frontier Foundation, accessed February 15, 2015, https://www.eff.org/https-everywhere.
9. "FAQ," InformAction, accessed February 15, 2015, https://noscript.net/faq#qa1_11.
10. "Atlas," Tor Project, accessed February 15, 2015, https://atlas.torproject.org.