2015

Radical Librarian-Technologists

John Schriner
CUNY Lehman College

Radical Librarian-Technologists

Schriner, John

Lehman College, City University of New York, US

ABSTRACT: Librarians may be finding themselves in the role of the technologist that supports students and faculty in Internet security, censorship circumvention, and supports whistleblowers and journalists. This paper looks at three cases where librarians present and teach technologies with these aims: the Tor anonymity network, secure communication in the field of journalism, and the librarian's place in the maker/hackerspace movement.

Keywords: technology; librarianship; censorship; journalism; privacy

Journal of Radical Librarianship, Vol. 1, pp.9–15. Published 1 May 2015.

The role of the academic librarian continues to change. It seems that there has been no better convergence of academic departments around technology than at this moment: the librarian speaks with journalism students about secure communications and privacy tools; to computer science faculty and students about setting up anonymity network relays to give censored users a voice; to student groups to help rein in unconstitutional surveillance. This article looks into three of many projects and why I believe librarians should take these on. First, the Tor anonymity network and how librarians can strengthen it. Next, encryption and journalism in a post-Snowden world. Last, the maker/hacker movement and where librarians fit in.

The idea of librarian as technologist is not new. Throughout the literature[1 2 3] the librarian is tasked and expected to learn computer skills and pass them on to students. The idea has even become in a sense "meta" as some librarians seek to Hack Library School and make it more useful.[4] Much has changed from early computer literacy days both in content and context, and there are still enormous challenges for librarians who provide one-shot information literacy and technology classes to students of varying computer skills. There is a need to teach Internet security and privacy in every level of education; for undergraduates it may be best to introduce basics such as avoiding being phished, the necessity of using HTTPS, using password managers. Some topics may be better understood by third and fourth year students, graduate students, faculty, and other librarians. Just as data librarians teach the use of Stata, or science librarians help chemistry students to use modeling software, specialized tools can be taught to specialized or niche audiences.[5] New specializations into other fields are no different in essence; the need for a librarian technologist to adapt and re-focus depending on the audience is certainly a good thing.

Academic librarians are often tasked with liaison to a department. The librarian conducts in-class instruction and one-on-one consultations because of their expertise in the tools in that field. As a liaison to the computer science department, this could mean assessing how we should both aid and encourage students to do research in socially beneficial areas of cryptography and, by that method, also propel the department's prestige[a] as a crucial part of a research institution.

Teaching Tor

The Tor anonymity network is used by millions of people to advance their privacy on the web.[6] Briefly, the Tor Browser Bundle bounces one's encrypted connection over three relays around the world before it reaches its destination. Relays may only see where the request is

---

a See the work of Stanford University's Applied Cryptography Group for their work in flash proxies (http://crypto.stanford.edu/) or Harvard's Berkman Center for Internet and Society for their work in law and social justice (http://cyber.law.harvard.edu/).

from and where it is going, so no single relay can see the full request.[b] By keeping one's IP address hidden, and by using a secure, hardened browser, the user may use the Internet anonymously in any country in the world. The Tor network allows users to tweet when Twitter is blocked, check Facebook when it is firewalled, and conduct research without worrying about who is watching their queries. Its more potentially inimical or controversial uses such as hidden services[7] [8] fall outside the scope of this paper but it is essential to stay current with this as well.

Tor development is research-driven. Tor Project supports researchers and academics by providing data sets, community-developed tools, and a large selection of the academic literature regarding the Tor network. New research is presented at practically every large technology or hacker conference worldwide. Lead developers also keep the community updated with their annual State of the Onion address.[9]

Setting up a Tor relay on campus is trivial but has many benefits.[10] The machine on campus simply serves as a middleman, passing encrypted traffic on a high-bandwidth network. Setting up a relay shows support for work in cryptography as well as showing support for human rights and liberation technologies. It is a proof-of-concept that faculty from different departments and librarians can work together on projects with far-reaching benefits. The benefits of supporting projects like these don't stop at the computer science department: the work of sociologists like Gabriella Coleman and Zeynep Tufekci begins to uncover trends and truths as social movements form that have unfettered access to social media and diverse strategies to meeting their goals. Ruminating on social movements leads to thinking about how journalism is changing: we look to technology, social media, and our immediate connection with events across the world and in our cities.

Librarian in the Newsroom

The world has been shaken by the revelations of government overreach whistleblowing in the past decade. The leaks by Chelsea Manning and Edward Snowden reveal U.S. government agencies that threaten privacy, and through weakening cryptographic systems[11] and creating backdoors, have made the Internet—and by extension the physical world—less secure. Librarians must work to help fix this error, starting with learning about encryption to help users stay safe on the Internet, and how to support whistleblowers.

Encrypted traffic ostensibly keeps agencies and individuals from snooping on Internet traffic. By learning more about how encryption, IP addressing, and secure communications work, librarians can provide this information in classrooms. In short, as Micah Lee of the

---

b Timing attacks can occur when the nation state or research team owns both the entry node and the exit node. Research into attacks on the network or the protocol is an important audit and welcomed by the Tor Project—of course as well as defenses to such attacks.

Electronic Frontier Foundation wrote, 'encryption works'.[12] It works to keep our personal correspondences private. Good encryption schemes rely not on trusting entities or developers but instead trusting the math, trusting the proper implementation of good cryptography. We use encryption every day: when we visit our email provider, or our bank, or an online retailer.[c] Naturally, strong encryption is essential to secure communication for journalists.

SecureDrop[13] (a forked project of the late Aaron Swartz now developed by the Freedom of Press Foundation) relies on the Tor network to keep sources' locations and identities obscured. The setup of SecureDrop is complex: it involves four computers and they need to be set up properly. The Freedom of Press Foundation offers technical assistance and training for journalists but librarians should also be guests in journalism classes to explain the architecture of SecureDrop and Globaleaks (another platform) and how/why we use them to protect sources. Encrypted email and chat best-practices should be familiar to journalists. Just one slip-up, one login from a personal machine or IP, can help to identify the journalist and the source. Further, librarians can offer the context and the concept of threat modeling that are necessary as foundations to secure communications.

Librarianship and journalism share a spot at the bedrock of democracy. The two fields are intrinsically connected by free speech and transparency.[14] [15] In New York City, public librarians at Brooklyn Public Library are leading the way in offering workshops called "Crypto for Journalists".[16] Cryptoparties[17] have been around since late 2012 alongside increased hacktivism[18] [19] [20] and the Arab Spring, but are just starting to make it onto workshop lists alongside "Photoshop for beginners." Cryptoparties teach the very basics of secure email, secure chats, and encrypted cellphone calls. Cryptoparties are not limited to this though—they give the community a space in which to adapt or specialize workshops and help each other to keep current with privacy issues and new technologies. This is a great step and it is just as important to learn how to stay safe on the Internet as it is to learn software skills.

Librarians in the Maker and Hackerspace Movement

Makerspaces[21] and Hackerspaces[22] abound all over the world now. These physical spaces allow for cryptoparties, social gatherings, robotics, 3D printing, crafting, soldering, etc. The Raspberry Pi (RPi) is a popular device at these spaces. The RPi is a low-cost Linux machine that boots from an SD card and can run on a battery. The library world has been abuzz about RPis as we think about different applications for these innovative little machines. Columbia University Libraries recently held an event to showcase ways to use RPis in the digital

---

c Some sites still don't use HTTPS by default. With a browser plugin like HTTPS Everywhere, our browser forces HTTPS and encrypts all the traffic so that computers "sniffing" the traffic can't see the data. Librarians ought to work with their IT department and make certain that plugins like this are installed on public workstations.

humanities, or as kiosks, or as mesh network nodes, or as site-specific libraryboxes.[23] It is no wonder that librarians feel at home in the maker movement: gadgets and new technologies like RPis are there to tinker with. There is potential for using RPis to further radical and humanitarian projects; from decentralized mesh networks that aid in censorship circumvention across cities, to providing Internet access and emergency response systems to rural areas. Using RPis and getting comfortable in the Linux environment is an important step to moving away from Windows/Apple closed-source operating systems. Besides the obvious benefit that Free and Open Source (FOSS) software is free (as in cost), it is also free (as in freedom to see or audit the source code, fork the project, or share the software). Healthy community-maintained projects offer support and often offer quick patches to vulnerabilities in the code. This transparency is antithetical to software such as Microsoft's Skype that loses the trust of the user when they offer backdoors to government programs.[24] The hope is that librarians advocate for open source software like they do for open access or open education resources. The ethos of this advocacy is the same: the model for closed-source applications (like closed, paywalled scholarly material) is essentially broken and we need to advocate for viable alternatives that are free and open.

The Maker and Hackerspace movement encourages, most of all, curiosity. This curiosity leads us back into the world of libraries when we find that the investigative tools[d] provided by the fields of digital forensics and penetration-testing gave us the information that Adobe Digital Editions was transmitting user information unencrypted to its servers from the client.[25] It is only through careful and thorough investigative work into library partners that we will keep these providers in check for user rights.

Conclusion

These three systems projects are linked with the foundational tenets of librarianship. Librarians have a passion for safeguarding privacy and free inquiry. Librarians are, by and large, curious and collaborative. Alongside instruction and the day-to-day interaction with users learning about Internet privacy, librarians need to stay current with new technologies and privacy issues. It is important that librarians network with other radical librarians at cryptoparties. At the time of writing, there are radical librarians working with the Library Freedom Project;[26] they are planning events for Radical Reference;[27] and they are planning cryptoparties at public libraries. Librarians need to be represented at technology, hacker, and maker conferences. As far as specific research needs: Tor research is the best way to improve the anonymity tool and understand how nation states attempt to block access.[28] [29] [30] For years now it has been a cat-and-mouse game but Tor stays ahead[31] because of its devoted

d Namely Wireshark, which is also useful for showing users the importance of HTTPS as opposed to easily-captured clear text.

developers, its prominence at conferences, and its obvious need worldwide. It is easy for librarians to get involved.[32]

Librarians are taking on the role of technologists for departments across campuses. As new methods for secure communication are developed, librarians will be there to provide teaching its usage. As new technologies help to further privacy, user rights, and unfettered access to the Internet, librarians will be there to support research, advocate, educate, and agitate. These are new roles for a librarianship that moves forward into uncharted waters. These are busy and exciting times for radical librarians.

References

1. Ruffin, Betsy. (2004). Librarian-Technologist: Ready for the Future. Library Media Connection, 22(7), 47.
2. Johnson, D. (2014). The librarian as technologist - what's our role? Library Media Connection, 33(3), 86. Retrieved April 29, 2015, from http://www.librarymediaconnection.com/pdf/lmc/reviews_and_articles/tables_of_contents/lmc_November_December_2014_toc.pdf
3. Boisselle, Juliet Habjan, Fliss, Susan, Mestre, Lori S., & Zinn, Fred. (2004). Talking toward Techno-Pedagogy: IT and Librarian Collaboration—Rethinking Our Roles. Resource Sharing & Information Networks, 17(1), 123-136. doi: 10.1300/J121v17n01_10
4. Hack Library School. (n.d.). Retrieved March 2, 2015, from http://hacklibraryschool.com/
5. Breeding, M. (2010). The systems librarian: Professional development for the library technologist. Computers in Libraries, 30(4), 30-32. Retrieved April 29, 2015 from http://www.librarytechnology.org/ltg-displaytext.pl?RC=14873
6. Tor Project: Anonymity Online. (n.d.). Retrieved March 3, 2015, from https://www.torproject.org/
7. Guitton, C. (2013). A review of the available content on Tor hidden services: The case against further development. Computers in Human Behavior, 29(6), 2805-2815. doi: 10.1016/j.chb.2013.07.031
8. Dr Gareth Owen: Tor: Hidden Services and Deanonymisation. (2015). Retrieved from https://www.youtube.com/watch?v=-oTEoLB-ses
9. State of the Onion [31c3] by Jacob Applebaum & Arma. (2015). Retrieved from https://www.youtube.com/watch?v=pRrFWwA-47U
10. Tor on Campus | Tor Challenge. (n.d.). Retrieved March 2, 2015, from https://www.eff.org/torchallenge/tor-on-campus.html
11. Schneier, B., Fredrikson, M., Kohno, T., & Ristenpart, T. (2015). Surreptitiously Weakening Cryptographic Systems (No. 097). Retrieved April 29, 2015 from http://eprint.iacr.org/2015/097
12. Encryption Works: How to Protect Your Privacy in the Age of NSA Surveillance | Freedom of the Press Foundation. (n.d.). Retrieved April 7, 2015, from https://freedom.press/encryption-works

13. SecureDrop | The open-source whistleblower submission system managed by Freedom of the Press Foundation. (n.d.). Retrieved April 21, 2015, from https://securedrop.org/
14. Is the Line Between Librarianship and Journalism Blurring? | American Libraries Magazine. (2011). Retrieved from http://americanlibrariesmagazine.org/2011/07/27/is-the-line-between-librarianship-and-journalism-blurring/
15. Goldsborough, Reid. (2010). The new age of investigative journalism? Teacher Librarian, 38(2), 57.
16. CryptoParty: Journalist Security Edition | Brooklyn Public Library. (n.d.). Retrieved April 7, 2015, from http://www.bklynlibrary.org/calendar/cryptoparty-journalist-se-central-library-info-comm-120814
17. [CryptoParty.]. (n.d.). Retrieved March 3, 2015, from https://www.cryptoparty.in/
18. The "hacktivists" of Telecomix lend a hand to the Arab Spring - The Washington Post. (2011). Retrieved April 21, 2015, from http://www.washingtonpost.com/lifestyle/style/the-hacktivists-of-telecomix-lend-a-hand-to-the-arab-spring/2011/12/05/gIQAAosraO_story.html
19. Anonymous and the Arab uprisings - Al Jazeera English. (2011). Retrieved April 21, 2015, from http://www.aljazeera.com/news/middleeast/2011/05/201151917634659824.html - Video interview with Gabriella Coleman (starts at 12:56)
20. Olson, P. (2012). We are Anonymous: Inside the hacker world of Lulzsec, Anonymous, and the global cyber insurgency. New York: Little, Brown and Co.
21. Directory. (n.d.). Retrieved from http://spaces.makerspace.com/makerspace-directory
22. HackerspaceWiki. (n.d.). Retrieved March 9, 2015, from http://hackerspaces.org/wiki/
23. Raspberry Pi: Presentation | Studio@Butler. (n.d.). Retrieved April 7, 2015, from https://studio.cul.columbia.edu/ai1ec_event/raspberry-pi-presentation/
24. Microsoft handed the NSA access to encrypted messages | The Guardian. (2013). Retrieved April 10, 2015, from http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data
25. Adobe's e-book reader sends your reading logs back to Adobe—in plain text [Updated] | Ars Technica. (2014). Retrieved April 7, 2015, from http://arstechnica.com/security/2014/10/adobes-e-book-reader-sends-your-reading-logs-back-to-adobe-in-plain-text/
26. Library Freedom Project. (n.d.). Retrieved from https://libraryfreedomproject.org/
27. Radical Reference | Answers for those who question authority. (n.d.). Retrieved March 3, 2015, from http://www.radicalreference.info/
28. Chaabane, A., Chen, T., Cunche, M., De Cristofaro, E., Friedman, A., & Kaafar, M.A. (2014). Censorship in the Wild: Analyzing Internet Filtering in Syria. arXiv:1402.3401 [cs]. Retrieved from http://arxiv.org/abs/1402.3401
29. Winter, P., & Lindskog, S. (n.d.). How the Great Firewall of China is Blocking Tor | USENIX. Retrieved March 4, 2015, from https://www.usenix.org/conference/foci12/workshop-program/presentation/Winter
30. Winter, P. (2014). Enhancing Censorship Resistance in the Tor Anonymity Network. Retrieved from http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A680558&dswid=4012

31. “Tor Stinks” presentation – read the full document | US news | theguardian.com. (2013). Retrieved March 2, 2015, from http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document

32. Tor: Volunteer. (n.d.). Retrieved March 2, 2015, from https://www.torproject.org/getinvolved/volunteer.html.en