Exploring the Dark Web: TOR for Activism

Tuesday, February 5, 2019

The Tor browser – often mistaken as being the "dark net" itself and seen as being synonymous with illegal or nefarious activities – has become a useful platform for activists who require privacy and anonymity, and one has been attracting increasing attention from activists and citizens alike in recent years. Tor is being seen as a potential tool for ensuring privacy in a world where the online activity of both activists and even everyday citizens are being closely monitored by corporate and state interests.

Surveillance technologies against activists

Source: https://www.shutterstock.com/image-photo/enter-darknet-294132083

Many activists now rely on social media platforms, such as Facebook, Twitter, Instagram, YouTube, to organize and mobilize for their cause. These platforms are widely relied upon by activists because of the low barrier to access, the potential to reach the millions of users locally and globally, and because they can be used to document protests and initiatives. As it turns out, these platforms are also heavily used by governments to monitor activists.

The use of surveillance tactics and technologies by police and governments to monitor everyday citizens has become increasingly commonplace1 since the attacks of September 11, 2001 (Taylor, 2011). This phenomenon of increasing state surveillance coincides with a period of significant political and civic mobilization and action – including the Idle No More, Occupy Wall Street, and Black Lives Matter movements – and with the development and widespread global adoption of digital technologies, including personal computers, smart phones and social media platforms.

Journalists have reported that the Department of Homeland Security consistently collected information of those attending protests from their social media platforms2, such as Facebook events set up to promote the protests, Twitter hashtags, Instagram and Vine feeds. Furthermore, journalists or everyday citizens taking photos of protests who post them on social media are providing further data for police to identify and surveil activists. The goal for these surveillance tactics over social media platforms were reportedly to "disrupt potential violence" (Patterson, 2017). However, as VICE points out, even without tagging an individual, Facebook uses a facial recognition algorithm that can identify people from facial images, putting everyone's privacy at risk (Rogers, 2016).

Social media platforms are not neutral, open spaces and it's clear that corporate interests do not align with activists needs. Social media design and policies are also often in tension with activist social media goals and needs (Dencik & Leistert, 2015; Van Dijck, 2013; Youmans & Work, 2012). While social media technologies "serve as venues for the shared expression of dissent, dissemination of information, and collective action" (Youmans & York, 2012, p. 315), the primary objective of social media companies, many of which are publicly traded companies and have fiduciary obligations to shareholders, is generating profit through advertising. Business models of these companies are built upon the mining of personal data about users, and keeping those users online as long as possible (Leistert, 2015).

TOR as an alternative and secure browser

The Tor browser provides an online alternative, allowing activists who have some technological know-how to use the browser as a means of organizing and mobilizing while remaining anonymous. Tor addresses concerns about privacy by letting activists encrypt their messages to one another, thereby mak-

ing it difficult to find out who is sending messages to whom. Tor masks your IP address (which identifies your location and then your potential identity) to prevent it from be used by governments to censor parts of the web. In this case Tor acts similar to a VPN but is volunteer-run, not subject to subpoenas, and does not keep logs of user traffic. For a VICE special on how to not get hacked, Jeong (2017) identifies major reasons why people would want to use the Tor browser. These are: trying to hide your identity, using public Wi-Fi, avoiding government censorship, and/or protecting other users of Tor as Tor becomes stronger the more people use it.

Although the Tor platform is often associated with the "dark web" based on the "darker" acts that occur using such encrypted communication technologies, as discussed in other parts of this issue, the anonymity of Tor has human rights and social justice implications. The "dark web" is often associated with the dangers that stem from its applicability for "dark" purposes such as criminal activity, buying and selling deadly weapons, illegal drugs, child pornography, ISIS communication, and White Supremacist communication. But the privacy and encryption offered by Tor are not just useful for criminal masterminds. These darker aspects are just a small percentage of what takes place on Tor. In response to Neo-Nazis turning to Tor for their continued mobilization (Hern 2017), leaders from the Tor Project explained:

> *We can't build free and open source tools that protect journalists, human rights activists, and ordinary people around the world if we also control who uses those tools …. Tor is designed to defend human rights and privacy by preventing anyone from censoring things, even us.*

Tor is neither "good" or "bad" just like the rest of the internet, however, what's important here is in how it is being used, who has access to this knowledge and who is often left out of the positive potentials of being anonymous online. As Jardine (2015) shows, the technology of the Tor platform can be used for both "darker" activities but also for democratic purposes. Data collected from Tor's network from 2011 and 2013 from over 157 countries demonstrate that although political repression drives most of Tor's usage (Jardine, 2018), in 2015, for instance, with over 2.5 millions users on Tor, only 40% of Tor's browser was used for nefarious purposes while 60% wasn't.

The anonymity of Tor provides users the benefits of organizing and communicating online with some safety from surveillance. The benefits of TOR are especially useful for those in countries with repressive governments that limit secure and private Internet access, and for those for journalists and activists to blow the whistle on corruption (Jardine, 2015). Examples of groups using these won't be that many because the whole point is for them to remain to be private. However, reporters have identified that Black Lives Matter activists moved over to using Signal and Tor to maintain privacy amongst the activists (Altman, 2015).

Tor, is, of course, not completely free from the risk of data and privacy breaches. There have been reports of security hacks and infiltration from the state and police that are concerning. Tor is left vulnerable through "weak links" in the computer network that is potentially logging more traffic that the node should be (Tor is hosted by volunteer computer nodes). This was how investigators were able to infiltrate ISIS communications (Roe, 2014). Police have also reportedly entered known child pornography forums, gathering information as a pretend pedophile. The FBI has also reportedly developed and used an application called Metasploit to identify users hiding behind Tor's browser (Poulsen, 2014).

But for now, Tor is still the better option than relying on VPNs, using WhatsApp Messenger for end-to-end encryption of messages, or even Signal, another popular application used for encryption and privacy while accessing and sharing online content (Jeong, 2017). The issues with many of these aforementioned applications in comparison to Tor is that they retain some metadata and, just like Facebook and Twitter, comply with data requests and court orders from government and local police authorities.

The TOR project

Because the Tor browser is funded through the US government and military but run completely by volunteers, it's hard to say how long the browser will survive given the trend of increasing state surveillance. And as more activists turn to Tor, technical limitations could pose challenges, including the need to handle the uptake of users while ensuring enough volunteer computers are in place to keep traffic secure.

The TOR Project, a non-profit organization that maintains the Tor software, is one example of a current initiative to expand Tor to everyone, beyond the criminal masterminds and spies that we often think of lurking in the dark depths of the Internet. The Tor Project wants everyone to be using it, so this shows us its capabilities as more than just a space where evil lurks. Using Tor effectively still requires technical know-how and access to the Internet, and in countries with repressive governments, such access to Tor may be hard to penetrate.

Donating to the Tor project, which began soliciting crowdfunding in 2015 (Russell, 2016), or becoming an active relay for computer nodes, are just a few ways to help ensure that the present and future of internet privacy is maintained for some of us until more of us demand action from our current browser and social media owners and more transparency from our governments in their interactions with them.

Lessons for everyone else

Corporate online surveillance is not just an issue that active protestors now need to worry about, but something that so many more of us are affected by in various ways. Recently, the report of Facebook's secret Cambridge Analytica scandal has fuelled the fire that non-consensual surveillance of users is common place (Chang, 2018). While the outing of such research studies has been a catalyst for improvement, with social media companies taking a more meaningful approach to educating users about privacy (Facebook and recent privacy notifications and suggestions to improve your privacy settings), users' data is still at risk given the legal authority of government authorities to access data through court order or through surveillance of digital technologies by agencies responsible for protecting national security.

Privacy is important for everyone who engages with online and networked forms of communication. Platforms like Tor help us to maintain our privacy to some extents. For activists engaged in social justice, this could provide a more secure way to organize and mobilize.

Works Cited:

Altman, A. (2015). "Person of the year, the short list: Black Lives Matter." In Time Magazine. Retrieved from http://time.com/time-person-of-the-year-2015-runner-up-black-lives-matter/

Chang, A. (May 2, 2018). "The Facebook and Cambridge Analytica scandal, explained with a simple diagram." In Vox. Retrieved from https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram

Dencik, L. & Leistert, O. (2015). *Critical perspectives on Social Media and Protest: Between Control and Emancipation*. Maryland: Rowman & Littlefield International.

Hern. A. (Aug 23, 2017). "The dilemma of the dark web: Protecting neo-Nazis and dissidents alike." In *The Guardian*. Retrieved from https://www.theguardian.com/technology/2017/aug/23/dark-web-neo-nazis-tor-dissidents-white-supremacists-criminals-paedophile-rings

Igo, S. (Apr 10, 2018). "How you helped create the crisis in private data." In *The Conversation*. Retrieved from https://theconversation.com/how-you-helped-create-the-crisis-in-private-data-94633

Jardine, E. (2015). "The Dark Web dilemma: Tor, anonymity and online policing." *Global Commission on Internet Governance Paper Series*, No. 21.
Retrieved from SSRN:https://ssrn.com/abstract=2667711orhttp://dx.doi.org/10.2139/ssrn.2667711

Jardine, E. (2018). "Tor, what is it good for? Political repression and the use of online anonymity-granting technologies."*New Media & Society*,*20*(2), 435-452.
Retrieved from https://journals.sagepub.com/doi/pdf/10.1177/1461444816639976

Jeong, S. (Nov 27, 2017). "The Motherboard guide to avoiding state surveillance." In *Motherboard by VICE*. Retrieved from https://motherboard.vice.com/en_us/article/a37m4g/the-motherboard-guide-to-avoiding-state-surveillance-privacy-guide

Leistert, O. (2015). "The revolution will not be liked: On the systemic constraints of corporate social media platforms for protests." In L. Dencik and O. Leistert (Eds.) *Critical perspectives on social media and protest: Between control and emancipation*. Maryland: Rowman and Littlefield.

Patterson, B. E. (Oct 19, 2017). "Police spied on New York Black Lives Matter group, internal police documents show". In *Mother Jones*. Retrieved from https://www.motherjones.com/crime-justice/2017/10/police-spied-on-new-york-black-lives-matter-group-internal-police-documents-show/

Poulsen, K. (Dec 16, 2014). "The FBI used the web's favorite hacking tool to unmask TOR users." In Wired. Retrieved from https://www.wired.com/2014/12/fbi-metasploit-tor/

Roe, K. (Nov 5, 2014). "Meet TOR: The misunderstood gateway into the Dark Web." In The Bottom Line. Retrieved from https://thebottomline.as.ucsb.edu/2014/11/meet-tor-the-misunderstood-gateway-into-the-dark-web

Rogers, K. (Feb 7, 2016). "That time the Super Bowl secretly used facial recognition software on fans". In *Motherboard by VICE*. Retrieved from https://motherboard.vice.com/en_us/article/kb78de/that-time-the-super-bowl-secretly-used-facial-recognition-software-on-fans

Russell, J. (2016). "TOR turns to crowdfunding to lessen its dependence on government money." In Techcrunch. Retrieved from https://techcrunch.com/2015/11/24/tor-turns-to-crowdfunding-to-lessen-its-dependence-on-government-money/

Taylor, A. (Sept 8, 2011). "9/11 The day of the attacks". In *The Atlantic*. Retrieved from https://www.theatlantic.com/photo/2011/09/911-the-day-of-the-attacks/100143/

Tor Project. (n.d.). "Tor project." Retrieved from https://www.torproject.org/

van Dijck, J. (2013). *The culture of connectivity: A critical history of social media.* Oxford: Oxford University Press.

Youmans, W. L., & York, J. C. (2012). "Social media and the activist toolkit: User agreements, corporate interests, and the information infrastructure of modern social movements." *Journal of Communication, 62*, 315–329. Retrieved from https://deepblue.lib.umich.edu/bitstream/handle/2027.42/91171/j.1460-2466.2012.01636.x.pdf?sequence=1&isAllowed=y

About the author

NASREEN RAJANI

Co-founder and organizer of the popular Women and Technology conference at Carleton University, Nasreen Rajani wants to bring scholars in the applied sciences and the social sciences and humanities from across Canada together to highlight scholarship on women and technology. Nasreen is a volunteer of the Women's Initiatives for Safer Environments (WISE), assisting the organization with their programming and communications planning. In 2013 and 2015 Nasreen presented about some of the crucial issues surrounding teen dating and social media as an invited keynote speaker for the In Love and In Danger conference with Family Services Ottawa. Her current PhD research focuses on how anti-harassment policies of social media platforms intersect with the increasing tension between freedom of online expression and online harassment of users. Nasreen secretly wants to live in a world where cake is normal for breakfast, her two cats always get along, and she's always dancing.

Nasreen Rajani is ALiGN researcher and writer.

Tuesday, February 5, 2019 | Categories: Illuminate, Issue I: Exploring the Dark Web
Post tagged with activism, Dark Web, Darknet, Digital Technologies, privacy, Surveillance, TOR
Share: Twitter, Facebook
Short URL: https://carleton.ca/align/?p=1684