(HTTP://WWW.FASTCOMPANY.COM)

Could The Road To The "Dark Web" Be The Right One?

As concerns about surveillance grow, browsing below the corporate and governmental radar may start to lose its underworldly taboo.

By Michael Grothaus (/user/michael-grothaus)

The NSA's secret surveillance program raised a number of issues regarding one's ability--and right--to remain anonymous on the Internet. For the web-savvy, navigating outside the purview of a corporate- and government-monitored Net required a special kind of web browser called Tor.

Tor has gotten something of a bad rap as a tool for guns, drugs, or human trafficking, and indeed many of the people that use the Internet anonymously may have things to hide. But Andrew Lewman, executive director of the Tor Project, says now's the time for everyday users to lose their trepidation and start browsing anonymously, no matter the present company.

An Internet For Drugs, Child Pornography, And Hitmen?

“No. I’m not into kiddie porn.”

That’s what a friend of mine says when I ask him if he’s ever used Tor.

When I ask another friend, she says, “That’s ‘The Dark Web,’ right? That’s Silk Road where you can buy guns and drugs and stuff? No, I’ve never used it, but I don’t need to have anyone killed right now.”

And, like my friends, if you have heard of Tor, which is also known by the shady monikers of “The Hidden Web,” “The Deep Net,” and “DarkNet,” you could be forgiven for thinking “Tor” equals “hangout for murderers, child pornographers, and drug dealers.” You could also be forgiven for linking Tor with guys like Dread Pirate Roberts (https://en.wikipedia.org/wiki/Silk_Road_%28marketplace%29), the operator of Silk Road, the online marketplace for guns and drugs and trafficking victims.

But that wouldn't quite be fair, says Lewman when I tell him my friends' impressions.

“Does your friend use a smartphone? How about cars? Kitchen knives?" Lewman says. "Then he's using the same tools as child abusers, terrorists, and other criminals. Technology is agnostic--the morality is in the human using it.”

The misconceptions about what Tor is are enormous. Tor is not a website, nor is it affiliated with the Silk Road, which was shut down by the FBI this October. It's more like... the safest road to the Silk Road.

“Silk Road is a funny situation,” Lewman says. “In some circles, it's a horror show of how drugs have permeated our culture. In other circles, it lets people safely get their drugs without having to resort to sketchy people in sketchy parts of the city.”

Many people are surprised to hear that the Tor Project is an authentic nonprofit that gets its funding from, among other sources, the U.S. and Swedish governments, not to mention that it originally grew out of an onion routing project (https://en.wikipedia.org/wiki/Onion_routing) run by the U.S. Navy.

Tor, like life--and the Internet we are all used to--is what you make of it. On the client end Tor is a simple browser that runs on most desktop operating systems that allows users to access a second Internet. This is a peer-to-peer Internet of anonymous, interconnected computers that make finding the true location or identity of a user virtually impossible. But while it’s true that this anonymity has led some people and organizations to set up shady websites that allow you to buy all kinds of illegal wares, that’s only because those people chose to use Tor to do that. Another group of people could very well choose to make a Tor website that delivers free puppies to lonely orphans.

“The hidden Net is no different than the Internet in the early 1990s,” Lewman says. “The original pioneers using the Internet were criminals and pornographers trying to figure out how to make money with it. And then came everyone else. This is the same situation we're in now, where early adopters are exploring the hidden networks

and figuring out how to make money or just exist within it."

But those early adopters many not be alone for much longer. While for many a second Internet may have seemed like an unnecessary complication just a year ago, the revelations of the existence of the NSA's PRISM program and the reach governments now have into hacking virtually anyone's personal information have brought the idea of a new Internet that, first and foremost, protects an individual's privacy and anonymity to the forefront of the "average" user's mind. PRISM also serves as a cold wakeup call for anyone who's ever thought privacy has existed on the web we've been using since the mid-'90s.

On The Internet, Everyone Knows You're A Dog

In 1993, the *New Yorker* published a cartoon by Peter Steiner that showed a dog sitting at a desk in front of a computer. The dog at the desk is addressing another dog sitting on the floor. He says, "On the Internet, nobody knows you're a dog."

The cartoon was the *New Yorker*'s most reprinted cartoon ever and conveyed the sense of total anonymity users felt they had on the then-new global communication platform that would carry the world into the 21st century.

The only problem, according to Lewman, was the *New Yorker*'s cartoon was a fallacy.

"The Internet is not private. It never has

been. Just because you don't use your name doesn't mean you aren't giving up intimate details of your life just by browsing around. The *New Yorker* furthered this misconception," Lewman says. "In fact, everyone knows you're a dog, what you like to read, buy, and post, and where you live. They then correlate that with offline data and have a complete picture of you. The 'they' can be advertising, marketing, surveillance, security, or e-commerce companies. Then there's the government-related 'they' in law enforcement, intelligence agencies, et cetera."

I think it would be foolish to assume that in 2013 most people don't think corporations like Facebook and Google and Amazon aren't tracking our anonymized Internet presence--where we go, what we click on. Taken to the next level, even when it became public knowledge that the U.S. government had the technology to spy on all of our online activity at any time, the public outrage quickly died down and people returned to their busy lives. The average person's attitude became, "So what? What am I going to do about it?" or "Why should I care? I'm not a terrorist."

But people should care, because the lack of Internet privacy and security cannot only be used against terrorists and those doing harm in the world. It can be used against political dissidents, journalists, and activists--in other words: people who generally work anonymously, for a period of time, to make the world a better place.

And that's why Tor, the perception people have of it, and the continued expansion of its user base is so important. It allows

political dissidents, journalists, and activists--many of whom use Tor just as frequently as arms and drug dealers do--to communicate safely, securely, and anonymously.

But the fact is most of us aren't political dissidents, journalists, and activists. Perhaps that's why the public outrage over PRISM has died down so much, because many are at ease that a "good" government (and I do realize that's a very relative description) like the U.S. is in charge of PRISM. But if the U.S. can do it, China can do it. And in the future many other less savory governments will be able to look into their citizens' lives at any time. And that's a very bad thing. After all, who's to say there won't be another controlling party like the Nazis in a hundred year's time running the U.S. or any other country? How many more Jews would have died in Nazi Germany if the Internet was the communication tool of choice back then and the government could see into anyone's lives at will? What if a government of the future decides anyone who has ever bought a left-leaning book from Amazon is a political threat and needs to be rounded up and eliminated?

The Future Of Internet Privacy

What a future evil government could do with the technological capabilities of PRISM is, of course, theoretical and perhaps best left to dystopian thinkers. However, just because some implications seem farfetched doesn't mean technology like Tor that could make us less surveillance-prone shouldn't be explored by the general public.

But for all the anonymity protections Tor has built in, that doesn't mean it's the final solution to anti-PRISM security, something Lewman readily admits.

For true anonymity, Lewman says users shouldn't solely rely on Tor; they must also be willing to change a number of their Internet usage habits (https://www.torproject.org/download/download-easy.html.en#warning). He also says that governments aren't the only threat, noting that no matter what the public face of a company proclaims, the big tech giants should not be trusted. "Unless it's free software you can have examined, one shouldn't trust them. People need to understand what they're giving to third parties when using them. Third parties could start being far more transparent about what they do with your data. Google is leading the way here, but everyone still has a long way to go."

As for mutual trust, I ask Lewman if any government agency has ever asked him for a back door into Tor. He tells me "no" and says that if any government did ask, his lawyers are confident they could fight the request in court and win. As for the NSA attacking Tor directly, Lewman says that despite a leaked NSA slide from 2007 saying the agency had no way to de-anonymize Tor, he can't be sure that's still the case. "No idea," he says. "Likely, no. We know they are trying to attack the browser and the user, not the encryption and Tor itself."

These constant back-and-forth battles over government surveillance, along with constant pressure from technology

companies, many of whom's business plans rely on us sharing our likes, purchase habits, and even feelings, makes the future of anonymity on the Internet seem bleak. But Lewman says it's important people don't give up.

"Anonymity has always mattered because anonymous speech is critical to a functional democracy," he says. "As speech moves online, so should the anonymity, if needed. People who want to sharecrop for large corporations can make their own decisions. The ability to have a choice to speak in your name or not means we're still doing something right."

As for the future of Tor, in light of the NSA revelations and the social sharing overload many of us are feeling, does Lewman feel that the world is ready for a second Internet, and do we (adapting Thomas Paine's words for the digital age) have it in our power to begin the web over again?

"Yes," he says. "Between the copyright cartels, data aggregation companies, and now governments spying and stalking on users, people are already looking for alternatives. We're at the beginning of a new wave of privacy-enhancing technology coming into the mainstream. The first ones to make it easy, sexy, and profitable will lead the way."

[Image: Flickr user Steve Corey (http://www.flickr.com /photos/stevecorey/11294949524/in/photostream/)]

MICHAEL GROTHAUS

I cover the stories behind the people and companies that make news in the tech

(http://www.fastcolabs.com/user/michael-grothaus)

world. I have a keen interest in any tech related to publishing, personal health, and the effects of mass media on our psyches. Outside of Fast Company I'm a novelist, journalist, published author and former screenwriter. I'm represented worldwide by The Hanbury Literary Agency in London.

Continue (http://www.fastcolabs.com/user/michael-grothaus)

December 10, 2013 | 12:42 PM

YOU MIGHT ALSO LIKE

Ellen Page Is Naked In The Uncanny Valley
Co. Design

(http://www.fastcodesign.com/3020630/ellen-page-is-naked-in-the-uncanny-valley)

Twitter's R.&D. Spending Hits the Right Spot
The New York

[?]