ESSAI

Volume 15 Article 13

Spring 2017

Enter the Hidden Dimension Behind Your Screen: The Deep Web

Tessa Burker
College of DuPage

Enter the Hidden Dimension Behind Your Screen: The Deep Web

by Tessa Burker

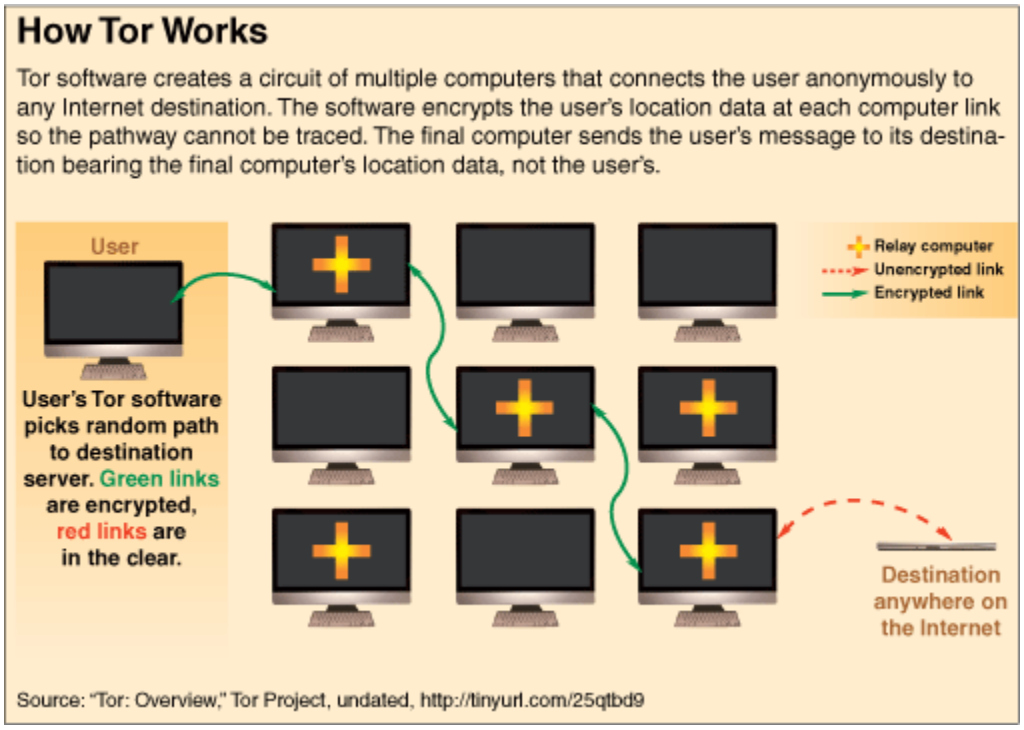
(English 1102)

So many films and works of literature are based on the idea that there are other dimensions--hidden worlds and unexplored land external to the bubble of world with which we surround ourselves. Ordinary characters just like you and me voyage to beautiful, fascinating lands. Often, we wish to ourselves that we were in those characters' shoes, treading on ground untouched by others. What if there was another world, a secret dimension that we know exists and can be explored, within our computer screens? Many of us surf the Google waves with little thought to the fact that our searches are monitored, recorded, and hardly private. But what if there is a way to evade such surveillance and anonymously browse the Internet? Many don't even know that such a thing does exist. This dimension exists within the Deep Web. As it is unfamiliar territory to many, it seems suspicious; having this anonymous way to browse the Web even seems dishonest. Some people argue that this dimension of the Internet is nothing more than a shady breeding ground for crime, producing criminals like a swamp produces mosquitoes. However, restricting the Deep Web or worse, abolishing it, infringes on freedom, violates privacy, and destroys a valid way to expose corruption. While illegal activities indeed happen on the Deep Web, it is necessary to realize that the benefits far outweigh the disadvantages.

The realm of the Deep Web includes anything on the Internet that cannot be accessed by standard search engines. As a whole, it is enormous. Although it is difficult to pinpoint exactly how much of the Internet is the Deep Web, some estimates put it at about 500 times larger than the Surface Web. This means that those thousands of "hits" you get from a simple Google search are only coming from a tiny portion of the Internet that is indexed for search engines. As *The Hidden Web: A Sourcebook* says, "Even the most sophisticated searcher, no matter what search engine they use, is only touching the surface of the information available on the Internet because they are not able to search the Invisible Web" (Scheeren 2). The name "the Deep Web" itself is misleading, as it includes not only things only accessed by special anonymizing browsers (which it is better known for) but also research databases and private company information, which of course make up a much larger portion of it. These databases and myriads of other websites that are simply not indexed are fundamental parts of the virtual infrastructure of libraries and businesses that are most certainly not illicit. At this point in our journey through the Deep Web, we must make a vital and paramount distinction between the land of the Deep Web and the village of the Dark Web that lies within it.

Here we peer over the boundary fence to catch a glimpse of the Dark Web. The Dark Web is a small corner of the Deep Web that requires special software to disguise your personal information and location. Because of this attribute, it is lumped into the total sum of the Deep Web. The Dark Web is where the illegal activities happen on the Deep Web, but this does not encompass everyone's purpose for being there.

Some of the stigma about the Deep Web comes from the way users access it. Journeying from the Surface Web to the Deep Web requires a bridge to cross the chasm; either a special link, a login, or a specific browser. The Dark Web is the section of the Deep Web that requires anonymizing software to disguise the location of the user. Tor is the most commonly used software to achieve this.



(Clemmitt)

Tor promises almost completely private Internet use. Of course, this comes with a downside. Because the users of Tor are anonymous, it is commonly used for criminal activity. Since everything on the Surface Web can be traced, it is much easier to find someone trying to sell marijuana there than in the Deep Web. With IP addresses and cookies, finding someone trying to commit crimes on the surface web may seem to be like peering through a clear pond and seeing straight to the bottom, rather than the suspicious, murky waters of the Deep Web. The waters of the Surface Web, however, are not crystal clear. Imagine how many emails must be sent a day through the Internet. Now suppose that in the masses of emails, a criminal wants to give a partner criminal a location for an illegal exchange of drugs for money. If the police are trying to trace the criminals to make an arrest, they would have to search through myriads of junk mail, party planning, business e-mails, and "Happy Birthday" e-cards from someone's grandma. It doesn't take a smart criminal to know that emails can be traced, so they would also use a code to exchange the necessary information. They are unlikely to be discovered, considering all the work it would take to find the correct e-mail and decipher the code. There are private e-mails on the Deep Web, but there are far, far fewer than on the Surface Web; even criminals who are aware of its existence know that it is much easier and safer to use the Surface Web to exchange information.

Not only is it often safer to hide amongst the millions of Surface Internet users, but also crime on the Internet exists with or without the Deep Web. As far back as 1971, college students with access to the fledgling Internet made the first online drug sale when they sold marijuana to other university students across the country (Clemmitt). Although some argue that these people would not even be criminals without this anonymous path, few are technically savvy enough to successfully use the Dark Web without a trace. Also, the Dark Web is certainly not immune to the law.

Take the classic example of the infamous Silk Road. The Silk Road was the main drug marketplace in the Dark Web village, facilitating about 1.2 million transactions in the two years it was open before it was shut down by the FBI. Ross Ulbricht, who operated the Silk Road under the name "Dread Pirate Roberts," was sentenced to life in prison without parole (Anderson and Farivar).

Using these anonymous Deep Web browsers and websites didn't disguise Ulbricht perfectly enough to allow him to infinitely succeed with his crimes. Even though this all happened on the Deep Web, going under the Surface Web radar does not guarantee successful crimes.

The very existence of the Silk Road makes getting drugs on the Deep Web seem incredibly easy, but there is a price for the convenience of anonymity. "Drugs on the Dark Net" goes into some detail about this:

> The resilience afforded by nodal redundancy does, however, come at a cost. As with any form of commercial enterprise, nodes that operate within an illicit distribution network must be compensated in some way for their participation. One way in which this compensation is achieved is by each node imposing a financial impost or 'mark-up' on an illicit good before it is passed on to a subsequent node. At every point of transaction within a supply chain, some form of price increase is likely to be imposed on the illicit drug which is then retained by each distributing node as profit. In principle, this process is no different from the price increases witnessed across legitimate supply chains, with the exception that there are relatively higher risks associated with illicit drug distribution (e.g. arrest, violence) which add a further premium to each price increase (Martin 53).

Buying drugs on the Dark Net is certainly costlier and riskier for the dealers, discouraging many from using this "easy" route to sell and acquire drugs.

Another argument made against the Deep Web is that it is used for child pornography. Alternatively, an important point is that there are far more other websites on the Deep Web than child pornography. Not only is the Deep Web so much more than the tiny portion that contains child pornography, but also far more child porn websites exist on the Surface Web. It seems that crime on the Internet will exist with or without private Internet browsing. Overall, while the Deep Web inevitably facilitates some crime, it is also heavily patrolled by law enforcement who are fully aware of this. Although it is easier to stay shrouded under the hood of the Deep Web, many have also been caught.

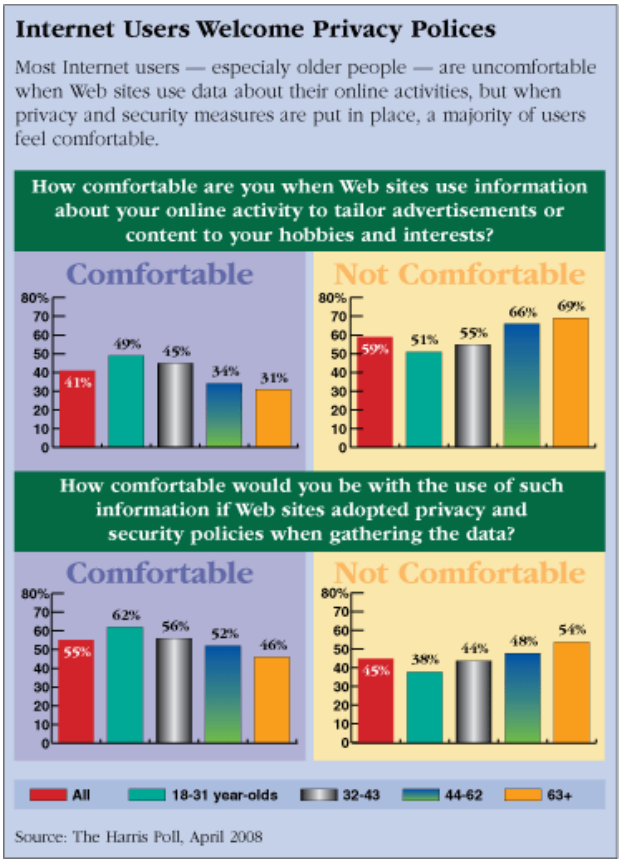
On the flipside, shutting down the Deep Web would destroy the important benefits of it. Deep Web browsers such as Tor allow users to anonymously search the Internet. Even though this way of browsing the Internet seems underhanded, most voyagers through the paths of Tor are merely searching the web anonymously wishing to protect their own privacy. One part of *The Googlization of Everything (And Why We Should Worry)* says, "If you read the privacy policy carefully, it's clear that Google retains the right to make significant decisions about our data without regard for our interests. Google will not share information with other companies without user consent, but it asserts the right to provide such information to law enforcement or government agencies as it sees fit" (Vaidhyanathan 85). Furthermore, in the article "Online Privacy," it says,

> What's more, powerful new technologies are creating unexpected challenges to privacy online. Advertisers, for example, can now track the Web sites you visit, and actions you take on those sites, to analyze how to more effectively sell products to you. And they may sell the information they collect to others. Privacy advocates, and some lawmakers in Congress, say the growing threats to online privacy point to the need for stronger laws to protect users' data. But Republicans in Congress warn that overregulation may cripple the economic foundation of the Internet (Marshall).

Of course, internet privacy advocates are extremely displeased with this and are roused to use an alternative where they feel they will not be tracked and watched. They feel that allowing themselves

to be traced on the Internet gives large companies a certain power, and they prefer to keep their browsing habits private.

Within the lore of the internet lies one landmark case discussed in "Privacy and the Internet." A Spanish man named Mario Costeja Gonzales discovered that Googling his name brought up an old article about how his house was for sale as a result of unpaid taxes, despite this debt having already been settled. When the company refused to remove the article, Gonzales sued Google, arguing that he should be allowed to demand that things defaming his name be removed from the Internet. The EU's highest court ruled in his favor, saying that in the EU an individual's right to privacy overruled any public interest in it (Glazer). Google allowing such a thing to exist simply for commercial purposes is one example of why people are driven to use private browsing over using a standard search engine; a protest against such behavior for moral reasons (not to mention for personal protection). In fact, more people are concerned about this than you may realize, as demonstrated by this chart's organization of how safe people feel on the Internet.



(Glazer)

With the Internet still being a fairly recent entity, it makes perfect sense that the older generations are especially nervous about privacy on the internet. However, it is easy to see that all ages show concern for their safety and privacy on the internet, as they rightfully should. Horror stories of stolen credit cards and identities are as common as words in a dictionary, not to mention the stories of pedophiles and stalkers looking for children and teenagers. Many do not even consider that their simple Google searches are not private to greedy companies.

One of the most well-known supporters of Tor and private Internet browsing is Edward Snowden. The hefty tale of Edward Snowden is a heterogeneous mix of good and bad. He only

worked for the NSA for a month before becoming greatly disturbed by its invasion of privacy. One day, he called in sick to work but instead fled the country. He flew to Hong Kong with a large collection of secrets. He gave a few carefully chosen reporters just a small portion of his collection of stolen information about the NSA. What these reporters revealed about his finding shocked the world. He revealed that the NSA had not only tapped thousands of phone lines, but also hacked into hundreds of thousands of Internet communication systems. Snowden disappeared and then reappeared in Russia, who agreed to grant him sanctuary. From there, he demonized the U.S. government, saying they had deliberately trapped him in Russia by invalidating his passport. The ripples Snowden caused affect the world today, four years later. The largest negative effect was a loss of faith in the government from the general population. It also revealed the government's legitimate attempts to help its citizens through learning about terrorist attacks with surveillance. It exposed the technology the NSA used to intercept communications to other nations. However, Snowden's revelation also did have some benefits. It revealed that the NSA was collecting phone records of hundreds of suspected terrorists. Although the terrorists were foreign and not domestic, their calls into the United States were monitored. Snowden argued that their vast collection of phone records could be used wrongly. He currently remains in Russia. While many of his supporters believe he should be pardoned, this is unlikely due to the massive damage his revelations did to the government (Epstein). An article on newsweek.com goes into great detail about this.

> Whether Snowden's theft was an idealistic attempt to right a wrong, a narcissistic drive to obtain personal recognition, an attempt to weaken the foundations of the surveillance infrastructure in which he worked, or all of the above, by the time he stepped off that Aeroflot jet in Moscow, it had evolved, intentionally or not, into something much simpler and far less admirable. He was disclosing vital national secrets to a foreign power. Conjectures about Snowden's motives matter less than the undeniable fact that he was greatly assisted in his endeavors by powerful enemies of the United States (Epstein).

While Snowden definitely went too far, it reminds us of how little privacy we truly have. Private information can be so easily discovered. Surveillance and hacking goes on all around us and most of the time we forget what's going on behind the scenes. After working with the NSA and CIA for many years, it is little wonder that Snowden is a huge proponent of Tor and private Internet browsing.

Another important use for the Dark Web is to allow for a freer Internet in countries with heavy regulations of the Web. For example, in China, the heavily restricted Internet is referred to as "The Great Firewall of China." It limits freedom of speech on the Internet as well as blocking certain searches and websites from its citizens. In the *New York Times*, one author goes into great detail discussing how censored and controlled the Internet of China is. "The government's firewall technology has become ever more sophisticated, and the cracks in the firewall have gotten smaller. Nearly every day a new V.P.N. provider is shuttered, and it is harder and harder to find a reliable long-term option" (Xuecun). If someone in the United States searches "Tiananmen Square" on the Internet, the first results that appear all discuss the massacre of the citizens demonstrating for democracy, accountability of the government, and freedom of the press. Troops armed with heavy artillery murdered thousands of citizens gathered there. Most people immediately associate the name of the place with this event. However, if you search "Tiananmen Square" or related words on the Internet in China, it either gives an error message, saying the search violates laws and cannot be displayed, or in some cases merely shows a few dates and birthdays (Xuecun). Imagine living in such a place where your government tries to hide its dark past from you; in a country like the United States where freedom and truth are part of our core and our identity as a country, we should be

shocked at such a thing. The people of China deserve to know their own history. The fact that the government would try to hide its mistakes is deplorable. This is why the Dark Web is so important. In order to be sure that they are learning the uncensored truth, citizens of China must use methods to bypass the Firewall. The only way to sidestep such censorship of knowledge in China is to access the information through the Dark Net.

Here at the end of our journey, we can safely say that the Deep Web is merely a more discreet Internet, nothing to be afraid of. The Dark Web is a much more uncertain territory, and we must take caution before treading on its land. However, both must exist and even have many important uses. Between keeping your information private and preferring to not be monitored and recorded to help big companies, many who are concerned for their own safety online opt for a private browser such as Tor, which also allows access to the Dark Web. Although there is crime on the Dark Web, it is not significantly greater than the amount of crime on the Surface Web and does not allow crime to run free. At the very least, the idea of the government and businesses having such easy access to personal information which they use for their own gain is disturbing; particularly in a country which trumpets freedom like the United States. The amount of Internet surveillance committed in the United States alone is disturbing. Safety online should concern all of us; we must work to ensure it for our fellow citizens. In the meantime, using a browser such as Tor does not indicate that the user is a criminal; most users of Tor are simply those concerned with privacy. While the Dark Net certainly has its shadowy corners, as long as there are those willing to violate our privacy, we must allow it to exist.

Works Cited

Albright, Dann. "6 Little-Known Corners of the Deep Web You Might Actually Like." *Make Use Of*. 4 February 2016. http://www.makeuseof.com/tag/little-known-corners-deep-web-might-actually-like/ .

Buying Guns and Drugs on the Deep Web (Documentary). Produced by Jasmin Steigler. Hosted by Tom Littlewood. Vice Media, 2013.

Clemmitt, Marcia. "The Dark Web." *CQ Researcher* 15 Jan. 2016: 49-72. Web. 14 Mar. 2017. http://library.cqpress.com/cqresearcher/document.php?id=cqresrre2016011500&type=hitist&num=0

Delamarter, Andrew. "The Darknet: A Quick Introduction for Business Leaders." *Harvard Business Review Digital Articles*, 09 Dec. 2016, pp. 2-5. EBSCOhost, cod.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=120606244&site=bsi-live.

Epstein, Edward. "Why President Obama Can't Pardon Edward Snowden." *Newsweek.com.* 5 January 2017. Accessed 6 May 2017. http://www.newsweek.com/why-obama-wont-pardon-edward-snowden-nsa-538632

Glazer, Sarah. "Privacy and the Internet." *CQ Researcher* 4 Dec. 2015: 1009-32. Web. Accessed 12 Apr. 2017. http://library.cqpress.com.cod.idm.oclc.org/cqresearcher/document.php?id=cqresrre2015120400&type=hitlist&num=2

Goodman, Mark. "Most of the Web Is Invisible to Google." *Popular Science.* 1 April 2015. Accessed 15 April 2017. http://www.popsci.com/dark-web-revealed

Kirkpatrick, Keith. "Financing the Dark Web" *Communications of the ACM*, vol. 60, no. 3, Mar. 2017, pp. 21-22. EBSCOhost, doi:10.1145/3037386. http://web.b.ebscohost.com/bsi/detail/detail?vid=4&sid=10f7b3b1-02d8-4225-aeea-050788a117e0%40sessionmgr104&bdata=JnNpdGU9YnNpLWxpdmU%3d#AN=121487469&db=bth

Marshall, Patrick. "Online Privacy." *CQ Researcher* 6 Nov. 2009: 933-56. Web. Accessed 12 April 2017. http://library.cqpress.com.cod.idm.oclc.org/cqresearcher/document.php?id=cqresrre2009110600&type=hitlist&num=3

Martin, James, and Palgrave (Firm). *Drugs on the Dark Net: How Cryptomarkets Are Transforming the Global Trade in Illicit Drugs*. Houndmills, Basingstoke, Hampshire, Palgrave Macmillan, 2014.

Scheeren, William O. *The Hidden Web: A Sourcebook*. Santa Barbara, California, Libraries Unlimited, an Imprint of ABC-CLIO, LLC, 2012.

"The Deep Web and Its Weird but Legal Hangouts." *Dark Web News*. 24 June 2015, https://darkwebnews.com/news/the-deep-web-and-its-weird-but-legal-hangouts/.

Vaas, Lisa. "FBI's Warrantless 'Hack' of Silk Road Was Legal, Prosecutors Claim." *Naked Security*. Sophos Ltd, 10 October 2014, https://nakedsecurity.sophos.com/2014/10/10/fbis-warrantless-hack-of-silk-road-was-legal-prosecutors-claim/.

Vaidhyanathan, Siva. The Googlization of Everything: (And Why We Should Worry) (1). Berkeley, US: University of California Press, 2011. ProQuest ebrary. 14 March 2017. http://site.ebrary.com/lib/codlibrary/reader.action?docID=10446271&ppg=97 (Chapter 3)

Xuecun, Murong. "Scaling China's Great Firewall." *The New York Times*. 17 August 2015. Accessed 6 May 2017.

Yeung, Peter. "A Tour of the Best, Entirely Legal Hangouts on the Deep Web." *Motherboard*. 22 May 2014, https://motherboard.vice.com/en_us/article/the-legal-side-of-the-deep-web-is-wonderfully-bizarre.