**Can we permanently shut down the dark web? Would we want to? Why or why not?**

<http://www.ibmbigdatahub.com/blog/what-dark-web>

No….maybe. If your speaking about TOR instead of the whole dark web - we can shut it down.

A few people have compared it to shuting down the internet but I think there are a **number of things that make it different**:

* It is really slow.
* It relies on relays, and those rely on people who are willing to spend time and money to keep it secure.
* Its continued development (and security) relies on volunteers and donation - and all of this is organized by one organization.

**How could we shut TOR down:**

* We could flood it with traffic.
* We could spread propaganda (true or untrue) and discourage or even criminalize helping keep TOR (and networks like it) operational - this effort would have to be global.
* We could break the organization that organizes TOR information and software and this would fracture development and versions, make it difficult to obtain TOR software, leave the network open to exploits.

A mixture of all of these tactics could cripple the dark net and if we applied this to other networks as well we may end the dark net.

Weather or not we should is another debate.

## **How to access the dark web**

Tor is the most popular dark web interface, with millions of users. There are a number of ways to access the Tor network, including via the [Tor browser](https://www.torproject.org/projects/torbrowser.html.en) , the [operating system Tails](https://tails.boum.org/), or by installing Tor on your computer. ProtonVPN also provides one-click Tor access through the [Tor over VPN feature](https://protonvpn.com/blog/tor-vpn/). From there, you can browse the web normally as well as gain access to highly private and secure onion sites.

Unlike the regular web, however, even after you have connected to the dark web, it isn’t so easy to find websites. Dark web sites use randomly generated domains that aren’t easy to remember. The dark web is also difficult to index, meaning search engines are ineffective. There are a number of link directories, such as The Hidden Wiki, that attempt to catalogue the dark web. But because dark web sites change their domain frequently, you’ll find a lot of dead links. A typical onion site url looks something like this:

http://3g2upl4pq6kufc4m.onion/

Some special onion sites, though, have easy to remember domain names and also SSL encryption (URLs that start with “https” instead of “http”). For example, [ProtonMail’s Tor](https://protonmail.com/tor) encrypted email site is at **https://protonirockerxow.onion** while Facebook’s onion site is at https://facebookcorewwwi.onion. You can learn more about these special onion sites [here](https://protonmail.com/blog/tor-encrypted-email/).

## **What’s on the dark web?**

The illicit uses of the dark web are well documented: assassination services, ecommerce sites for buying guns and drugs, and so on. It’s best to stay clear of anything that seems suspect while browsing there. However, there are plenty of 100% legal things you can do on the dark web. You can read [ProPublica](https://www.propublica.org/nerds/a-more-secure-and-anonymous-propublica-using-tor-hidden-services) or [The New York Times](https://open.nytimes.com/https-open-nytimes-com-the-new-york-times-as-a-tor-onion-service-e0d0b67b7482), [check your email in ProtonMail](https://protonmail.com/blog/tor-encrypted-email/), or [browse your Facebook wall](https://www.facebook.com/facebookcorewwwi). All of these mainstream websites offer dark web access because of the benefits to privacy and freedom of information.

One of the biggest advantages of the dark web is the difficulty of blocking it. Common forms of censorship, which block traffic to websites at specific choke points along the Internet hierarchy, do not work with encrypted overlay networks. (As a result, some dictators have, for example, [tried to block Tor itself](https://www.theverge.com/2018/6/25/17503680/venezuela-tor-blocked-web-censorship).)

For similar reasons, the dark web is more resistant to surveillance by governments and corporations (such as Internet service providers). Whistleblowers, journalists, and other professionals at risk of targeted surveillance use the dark web to communicate sensitive information. And organizations including Human Rights Watch and the Electronic Frontier Foundation support the use of and access to the dark web.

One of the only drawbacks of the dark web is its speed. For instance, because Tor bounces your traffic through multiple servers around the world, it necessarily slows your connection. But when you need it, the dark web can be vitally important: When [Turkey temporarily blocked ProtonMail for some users](https://protonmail.com/blog/turkey-online-censorship-bypass/), our onion site was one of the only ways people could gain access to email.

So, there’s no reason to be afraid of the dark web. On the contrary, the dark web is an essential privacy tool. As governments work to w[eaken encryption with backdoors](https://protonmail.com/blog/encryption-backdoor/) and [corporations gain greater access to everything we do](https://protonmail.com/blog/google-privacy-problem/), privacy and security technologies like the dark web must be vigorously defended. And that starts with understanding them beyond sensational headlines.

# Is Tor browser illegal?

Heavens no! The Tor Network was developed by a department of the U.S. government and it is used to assure private communications by government agencies. The privacy it provides does make it a valuable tool for some people who do use it to commit crimes. But there are perfectly legitimate reasons for anyone to use it. Fear not.

There are some very oppressive countries in which use of the Tor Network may be regarded as suspicious behavior. I don’t know if any have declared it illegal; but, depending on your government some caution might be justified.

Hi,

Smile before you read this. Life is really beautiful.

Now coming back to your question,

“Tor Browser is not illegal (except in some countries) These are the countries that are mostly and majorly against free internet. Now I won’t bitch about any of these countries as I don’t want this answer to be political. But yes, these Governments do want to control every inch of their public’s lives.”

But if you’re not living in China, or in some regions of Russia, or UAE, you need not worry about it. Even in these countries, people use it all the time. Mainly, the Tor Browser is infamous due to a somewhat presence of illegal market and buyers of such markets on the dark web.

But we can’t deny the fact that Tor Browser is one of the best ways of protecting and ensuring your internet anonymity and safe browsing.

I can go on and on, but I think you may be satisfied with the answer right? If not, just tell me, I have a great knack for writing and I’ll definitely write more if asked.

Oh and hey! I do know of an app which is 100% not illegal and offers both a TOR and a VPN (alright, don’t give me that smirk. It’s not a sales pitch. I really like the app)

Here’s a link to the app: [‎](https://apps.apple.com/bm/app/tor-browser-private-web-vpn/id1476914678)

Be sure to try it at least once. If you’re not comfortable with clicking on links, just type **TOR Browser Private Web + VPN** and install the one with a purple icon.

**TOR is not illegal to use. (in most world)**

However, using it to engage in illegal activities is illegal.

You see TOR was developed to ensure optimum privacy (if it exists) It masks your identity and bounces your data on 3 servers at least so that your activities are not only hidden but also untrackable. However, as it is with everything else, people started to use it for illegal and offensive activities. They exploit it and many Governments all over the world started imposing limitations on the use of TOR.

However, the limitations aren’t on the use use of TOR> It comes down to how you use it. Wiki leaks used the TOR browser to access restricted sites and sensitive data. This type of incident is what makes Governments wary of such privacy advancements.

Long story short, you can use TOR all you want (also consider your country’s policies about it) but as long as you’re using it to access meaningful content, you’re good to go.

**No TOR is not illegal… but you should know how to use it before you get into deep web.**

TOR (The Onion Router)

sites on the dark web or deep web use .onion as domain and to crawl through them we need special tools. One of such tools is TOR. It is basically an anonymity browser i.e it keeps your location unknown or at least safe as compared to regular browsers. It does so by encryption of data at the application layer of the communication protocol stack.in easy words,deep web contains much more data as compared to the surface net. But to access such data you need precautions as well as some special tools to crawl through the internet. And TOR consists of all these features.

I think this article will help you [TOR (The Onion Router) - Theanonymousguy.com](https://theanonymousguy.com/everything-about-tor-the-onion-router/)TOR browser is not illegal. It is an absolute rights of everyone to protect their identity.Using TOR is not risky when compared to normal online usage.It is become illegal or risky based on your activity. If you are using TOR to engage in illegal activities, then it is risky and illegal.