What is Tor?

Tor is short for “The Onion Router.” It is often viewed negatively by the press and law enforcement agencies, but it has many positive benefits. Journalists and their sources rely on it to communicate securely and anonymously, without fear of government interference. Secure communication is essential in [whistleblowing](https://www.expressvpn.com/blog/how-to-be-a-whistleblower/) cases, like the[Edward Snowden](https://www.expressvpn.com/blog/quick-biography-edward-snowden/) revelations. Similarly, Tor is important for law enforcement as it allows for covert operations and investigations online. Tor currently has about two million daily users worldwide, most of them originating from the United States, Germany, and Russia.

Similar to a VPN, you can use Tor to hide your[IP address](https://www.expressvpn.com/what-is-my-ip) and anonymize your internet traffic. Using the Tor Browser also allows you access to the dark web, and run a “hidden service” anonymously. Generally, the Tor Browser will not anonymize all your web traffic, which is why it is commonly run alongside a VPN.

Connecting to [Tor through a VPN connection](https://www.expressvpn.com/vpn-service/tor-vpn) is a great way to maintain your internet privacy and security. Not only will it hide your browsing data from your VPN company, it will also [hide your home IP address](https://www.expressvpn.com/what-is-my-ip/hide-my-ip) from the Tor entry node.

The unlikely history of Tor

Tor: The early years

The United States armed forces have always relied on a vast network of spies around the globe to gather information. As this information became increasingly digital in the 1990s, the agencies realized how valuable it would be for their assets to communicate online.

No longer would spies need bulky radios, or have to decipher messages in newspapers to receive information. But the U.S. military was also aware that the way[the internet](https://www.expressvpn.com/blog/what-is-the-internet/) was constructed posed serious threats to the identity and security of their sources. It would be very easy to detect who was communicating with servers operated by U.S. intelligence or military.

Imagine an NGO discovering one of their members frequently logs into the members-only forum of a military base, or a large corporation noticing that an employee is frequently opening up the website of a government agency. Without a global network providing anonymity, spies, police, and other government organizations wouldn’t be able to effectively communicate with their sources or carry out covert investigations.

In the mid-1990s, the U.S. Naval Research Laboratory began to work on a solution. They started to develop a way to route encrypted data through a network of computers placed all around the world. This routing method would hide both the origin and the destination of all the data. After 1997, the project was further developed by the Defense Advanced Research Projects Agency (DARPA).

But how would such a network authenticate its users? And how would such a network remain undetected? Who else could profit from being able to access the uncensored internet in an anonymous way?

### Public tool instead of secret weapon

We can wildly speculate about these questions, but for historians, it is difficult to determine what debates the military and intelligence organizations involved went through, and which arguments convinced them to release the software for public use, under a free license, in 2002. The responsibility to maintain the project was handed over to the[Electronic Frontier Foundation](https://www.eff.org/) (EFF), which then handed control to The Tor Project. The majority of its funds still come from the United States government, though the government of Sweden also[contributes significantly](https://www.expressvpn.com/blog/online-privacy-is-why-sweden-wins-the-internet/).

The reasons for the government’s involvement in the Tor Project might appear contradictory. The government wants to continue to use the Tor network to obfuscate the source of its attacks, to infiltrate civil rights movements, and to enable its spies to communicate intelligence securely and effectively. On the other hand, they gave the public a tool that would allow anyone to obfuscate the source of their attacks and hide, or information, from the government.

### With and against the government

But to be able to use this tool without raising suspicion, the government needs to promote the Tor network as a liberating and empowering technology for those who want to break free from authoritarian control. They needed to not just promote it by spreading the word, but also by making the software genuinely effective and endorsed by the same people the government wishes to gather information on.

The government needed to give up power to maintain power. This complicated balance is probably also the reason the U.S. government has made itself a name as both a vivid supporter and ferocious attacker of this technology.

Organizations like the U.S. government are not entirely homogeneous, and no doubt consist of actors who honestly try to protect civil rights, as well as those who wish to strengthen authoritarian structures.

Can a balance be struck between power and freedom?

To use the Tor network to our advantage, we must understand how it works and what the limitations are. Tor’s open-source code allows us to understand exactly what is going on under the hood and audit the implementation of secure encryption.

## How Tor works under the hood

Let’s pretend that computers and the internet don’t exist and people still communicate with what we now call “traditional mail.”

Now, say you want to buy a book. How could you do so without leaving the house? You could use the yellow pages to look up the address of a publishing house, then send them a postcard.

On that card, you could express a desire to obtain a book you like, and you could include your own address so that the publisher knows where to send it to.

The problem is that everyone along the delivery route can see what everyone wants to read. They can make copies of everything or simply keep lists of who requested what.

### Envelopes protect the content

A simple level of protection would be to put requests into sealed envelopes. These cryptographic seals are impossible to open without breaking them, so all the post office could do is maintain lists of what gets delivered where, without knowing the contents of the envelopes.

This information—pertaining to, for example, the size and weight of the envelope, and the identities of the sender and recipient—is called the[metadata](https://www.expressvpn.com/blog/metadata/).

Metadata reveals a lot. For example, you can tell if you’ve received a speeding ticket just from looking at the envelope. And so can the mailman.

This is very close to how the internet works today. Cryptographic seals go one step further by being impossible to open. In the past years basic[encryption](https://www.expressvpn.com/what-is-vpn/vpn-encryption), like Transport Layer Security (TLS), has become a standard across the web. (You can tell when this is active, as a lock icon will appear in your address bar).

### Tor circuits rely on a system of nodes

To send requests anonymously in the Tor network, you start by establishing a Tor circuit. To do this, you send your “sealed postcard” to a random Tor node. This could be a residential or commercial address. It could be your neighbor’s house, or it could be a big building in a faraway country. This is your **entry node**, and all your sealed mail will be sent to this address. All the mail that you receive will also come from this address.

Your entry node will forward your mail to yet another node, which will again forward it on to another node—the **exit node**. Only the exit node knows the address of your intended recipient.

The following is an explanation of how the system of nodes works:

* The entry node can see who you are, but not what you request or who you request it from.
* The middle node cannot see anything. It is important because it separates the exit and entry nodes from each other.
* The exit node can only see what you request, but not who you are. Ideally you will be using TLS to end-to-end encrypt your request, so the exit node can see who you are requesting something from, but not the content of your request.