

TorProject.org

## Tor's Mission

The Tor Project builds and distributes free tools that allow journalists, human rights activists, diplomats, business people, and everyone else to use the Internet without being watched online by governments or companies.

The Tor Project is also a global resource for technology, advocacy, research, and education in the pursuit of freedom of speech, privacy rights online, and censorship circumvention. The Tor Project is proud to be a leading 501(c)(3) nonprofit organization.

Learn more at  
<https://www.torproject.org/>



## Join Us

We need your help to continue this global work in the ongoing pursuit of freedom of speech, privacy rights online, and censorship circumvention. Join us as a sponsor, a volunteer, a funder, or for upcoming events led by the Tor team.

## What Tor Does Best

- Providing privacy online
- Defeating censorship
- Protecting journalists
- Protecting human rights defenders
- Protecting domestic violence victims
- Keeping global online channels of information open for all
- Working with policymakers
- Partnering with academic and research institutions



# Law Enforcement & The Tor Project

## How Tor Works

### Who Uses Tor?

The vast majority of Tor users are ordinary citizens who want to stay in control of their privacy online—or censored users who need to circumvent Internet blockage. Criminals who are willing to break the law already have more effective options than using Tor.

### No Logs, No Backdoor

Tor users can rely on the privacy of Tor. By design, a Tor relay operator or someone with physical access to a Tor relay cannot reveal a Tor user's IP address. Continual peer review of Tor's source code by academic and open source communities ensures that there are no backdoors in Tor.

### Anonymous Tip Lines

Tor provides the most secure infrastructure for a truly anonymous online tip line—critical in keeping channels of communication safe for witnesses and informants.

### Undercover Operations

Tor is used by law enforcement agencies and investigators to monitor the web pages and services of suspects anonymously. By hiding investigators' identities and locations, Tor can be a valuable tool for successful online undercover operations.



Alice encrypts her web page request to Bob three times and sends it to the first relay.



The first relay removes the first encryption layer but doesn't learn that the web page request goes to Bob.



The second relay removes another encryption layer and forwards the web page request.



The third relay removes the last encryption layer and forwards the web page request to Bob, but doesn't know that it comes from Alice.



Bob doesn't know that the web page request came from Alice, unless she tells him so.

## Learn More

- Tor's ongoing commitment to education includes law enforcement and policymakers.
- Tor's documentation and support channels are open to everyone.
- Learn how to use the ExoneraTor service to find out whether an IP address was used by a Tor relay.
- Learn more by reaching out to Tor's team of experts.



# The Benefits of Anonymity Online

## How Tor Works

### The Reality

Internet Service Providers (such as BT and Verizon), websites (such as Google and Facebook), and governments use a common form of Internet surveillance known as IP address tracking to monitor conversations over public networks.

- News sites may promote different articles based on your location.
- Shopping sites may use price discrimination based on your country or institution of origin.
- An average person is tracked by over a hundred companies that sell profiles to advertisers.
- Your social media activity can be revealed and used against you by malicious individuals.

### Freedom

The landscape of the Internet is in a constant state of change, and trends in law, policy, and technology threaten anonymity as never before, undermining our ability to speak and read freely online. Countries are watching each other as well as their own citizens, blocking websites, watching traffic content, and restricting important world news.



Alice encrypts her web page request to Bob three times and sends it to the first relay.



The first relay removes the first encryption layer but doesn't learn that the web page request goes to Bob.



The second relay removes another encryption layer and forwards the web page request.



The third relay removes the last encryption layer and forwards the web page request to Bob, but doesn't know that it comes from Alice.



Bob doesn't know that the web page request came from Alice, unless she tells him so.

## #1 in Privacy Online

- Tor is free, open source technology, honed over 10 years of research and development by Tor's team of security researchers and software developers.
- Tor is one of the most effective technologies to protect your privacy online and ensure your personal online security stays in your control.



# Freedom & Privacy Online

## How Tor Works

### censorship

(Merriam-Webster, 2012)

*Act of changing or suppressing speech or writing that is considered subversive of the common good.*

### Online Censorship

On a global playing field, censorship takes on a whole new meaning. Restricting access to information and monitoring outgoing content is more common than most people realize. The censorship researchers at Tor work to build tools that stay ahead of censorship tactics and provide open channels of communication for everyone online. The Tor team builds partnerships to raise awareness and educate people about the importance of privacy online and freedom of speech online.



Alice encrypts her web page request to Bob three times and sends it to the first relay.



The first relay removes the first encryption layer but doesn't learn that the web page request goes to Bob.



The second relay removes another encryption layer and forwards the web page request.

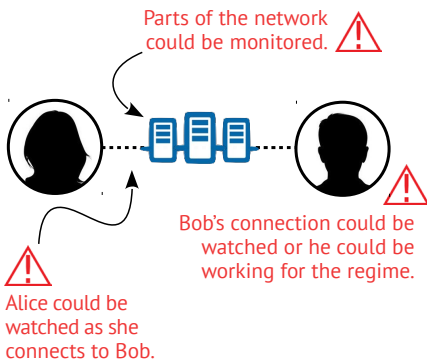


The third relay removes the last encryption layer and forwards the web page request to Bob, but doesn't know that it comes from Alice.

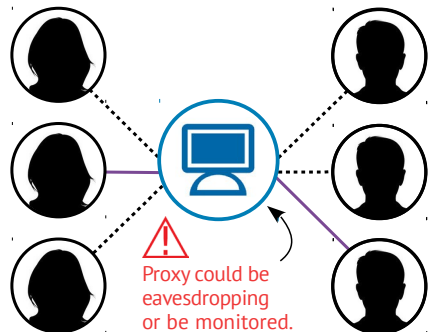


Bob doesn't know that the web page request came from Alice, unless she tells him so.

Internet surveillance is common and easy.



Some censorship circumvention designs use only one layer to hide connections.



Unfortunately, one layer (as with a proxy) is easy to attack.