ELECTRONIC FRONTIER FOUNDATION
PROTECTING RIGHTS AND DEFENDING FREEDOM ON THE ELECTRONIC FRONTIER eff.org

Tor: Myths and Facts

Tor is a service that helps protect your anonymity while using the Internet by obfuscating your online behavior and by obscuring your identity from unwanted surveillance from other users, governments, or corporations. When you use the Tor software, your IP address remains hidden, and it appears that your connection is coming from the IP address of a Tor exit relay, which can be anywhere in the world. Tor also allows access to .onion hidden services, which allow people to publish information while hiding their location.

Tor is comprised of two parts:

- ***software*** you can download that allows you to use the Internet anonymously (the Tor Browser Bundle)
- ***volunteer network of computers*** that make it possible for the software to work.

The Silk Road Case

The technology has come under scrutiny since the FBI shut down Silk Road, a website operated with a Tor hidden address that could be accessed through a computer running the Tor Browser Bundle. While some visitors of this particular website were primarily interested in the trafficking of illegal drugs, Tor users across the world have very practical and diverse reasons for deploying online anonymity.

X **MYTH: Tor is for criminals who want to make illegal transactions free from law enforcement's prying eyes.**

FACT: Tor is and can be used by anyone who would benefit from online anonymity: people who do not want companies to market to them based on their browsing data, individuals who live in countries with censored Internet access, journalists who need to protect their sources, or businesses that want to keep their strategies confidential. Without Tor, a user's location can be tracked whenever she goes online, and normal everyday Internet use creates an absurdly detailed profile of a user's whereabouts.

See how Tor and HTTPS work: eff.org/tor-and-https

✗ **MYTH: Tor does not provide protection from U.S. government surveillance because it was developed by the U.S. military and is funded in part by the U.S. State Department.**

FACT: The initial development of Tor was funded by the U.S. Navy, and the U.S. State Department currently funds Tor because the freedom-enhancing software is used to circumvent censorship in countries that block access to parts of the Internet. However, there is no evidence that the software includes a backdoor, and the code has been audited to look for vulnerabilities. All Tor projects are completely open-source and transparent in their design and implementation.

✗ **MYTH: Tor will completely protect one's online activity.**

FACT: The Tor software does not anonymize one's identity. It anonymizes where Internet traffic originates. While the government has been able to exploit vulnerabilities in out-of-date browsers to target Tor users and identify some Tor-related traffic, leaked government documents revealed that the core Tor technology continues to be a barrier to mass surveillance. Indeed, according to the NSA, "Tor Stinks." If someone on the Tor network does not want their identifying information to be found online, then she should use encryption and discretion in her emails, chats and other online communications, and keep the Tor Browser Bundle up-to-date.

EFF is a member-supported non-profit. Join today at eff.org/join

See how Tor and HTTPS work: eff.org/tor-and-https