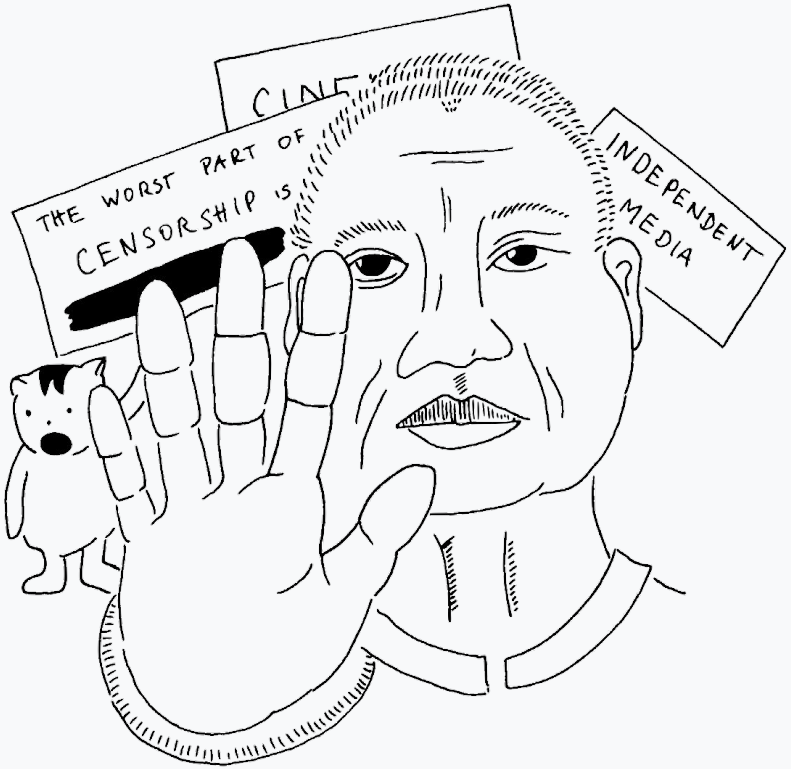
Bypassing Censorship With Tor

Updated: 20 March 2025



1.
How the Internet is Censored

Where Does Censorship Happen?

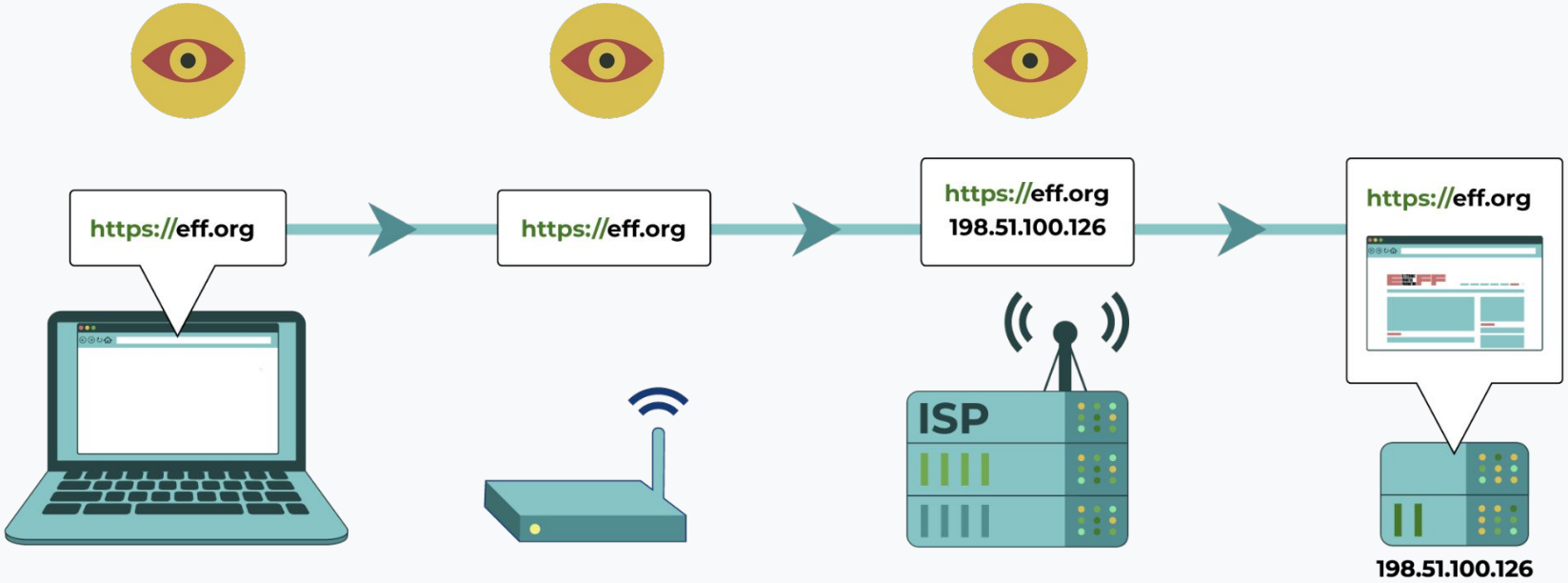
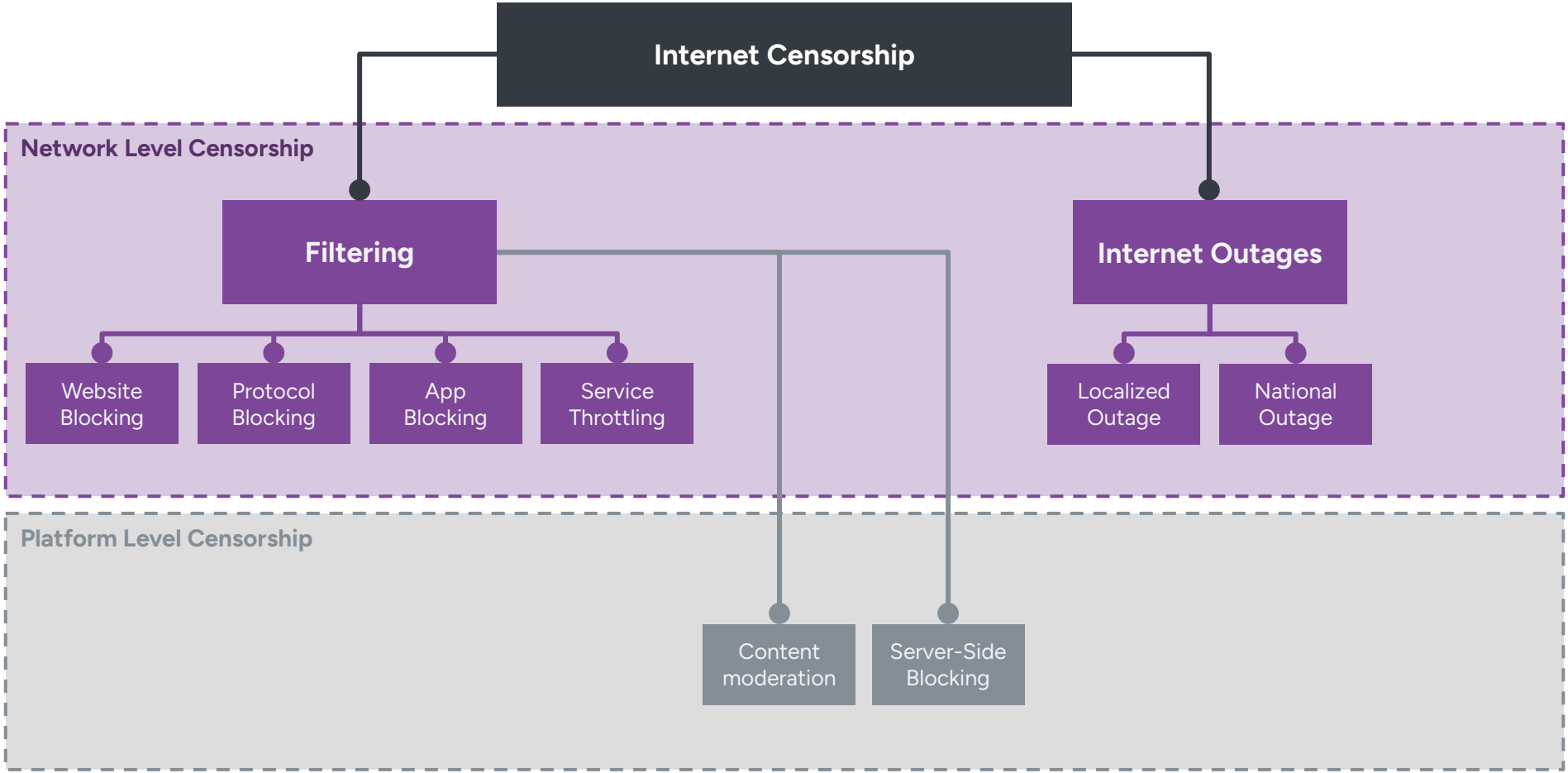
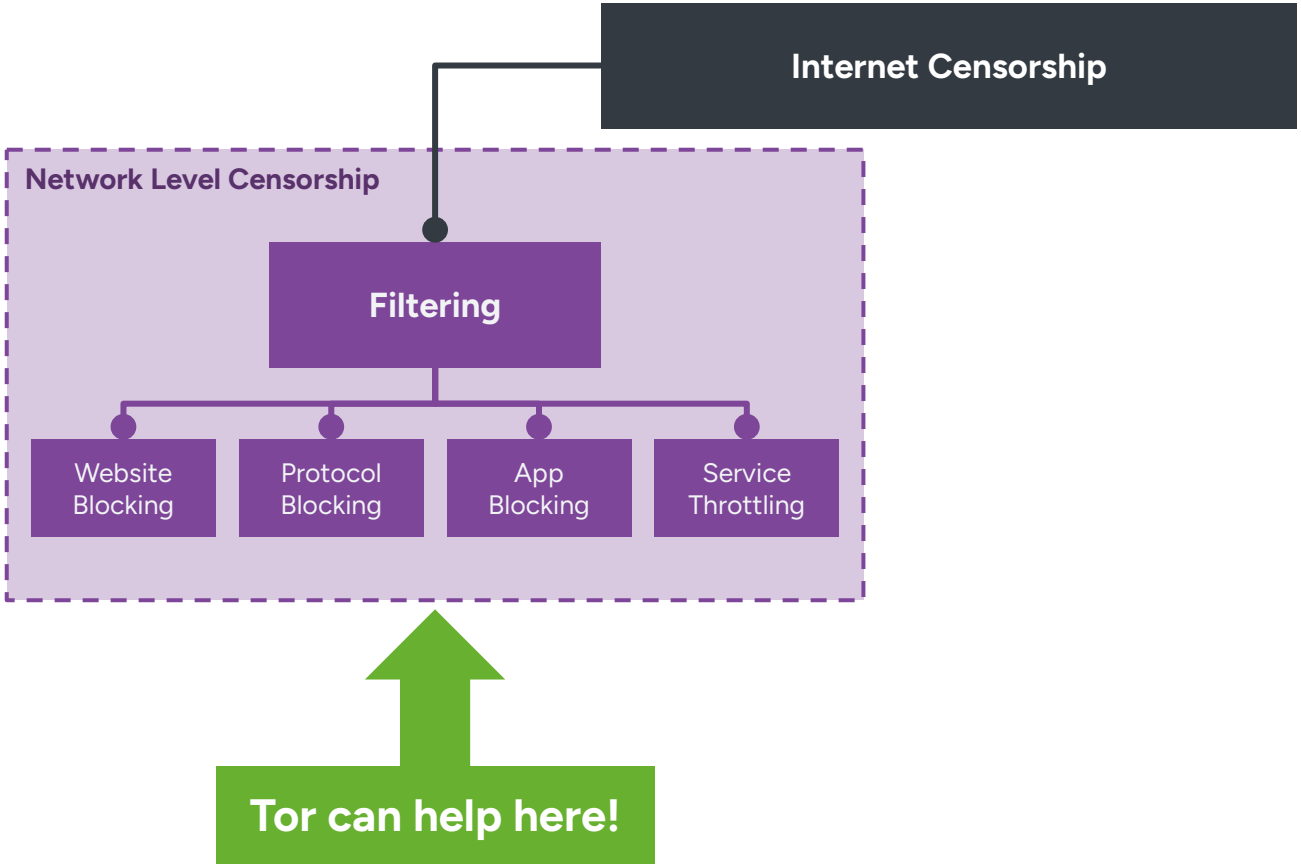


Image source: eff.org




Internet Censorship
Network Level Censorship
Filtering
Website Blocking
Protocol Blocking
App Blocking
Service Throttling
Tor can help here!

Two Sides of the Same Coin

- Censorship and surveillance go **hand in hand.**
- To block access to an online service (website or app), censors must first **detect** when users attempt to access it.
- To bypass this censorship, you need to **'mask' your destination**: first appearing to visit an unblocked location before proceeding to your intended website or app.

1.
Bypassing Censorship with VPNs vs. Tor

When Browsing the Internet Regularly

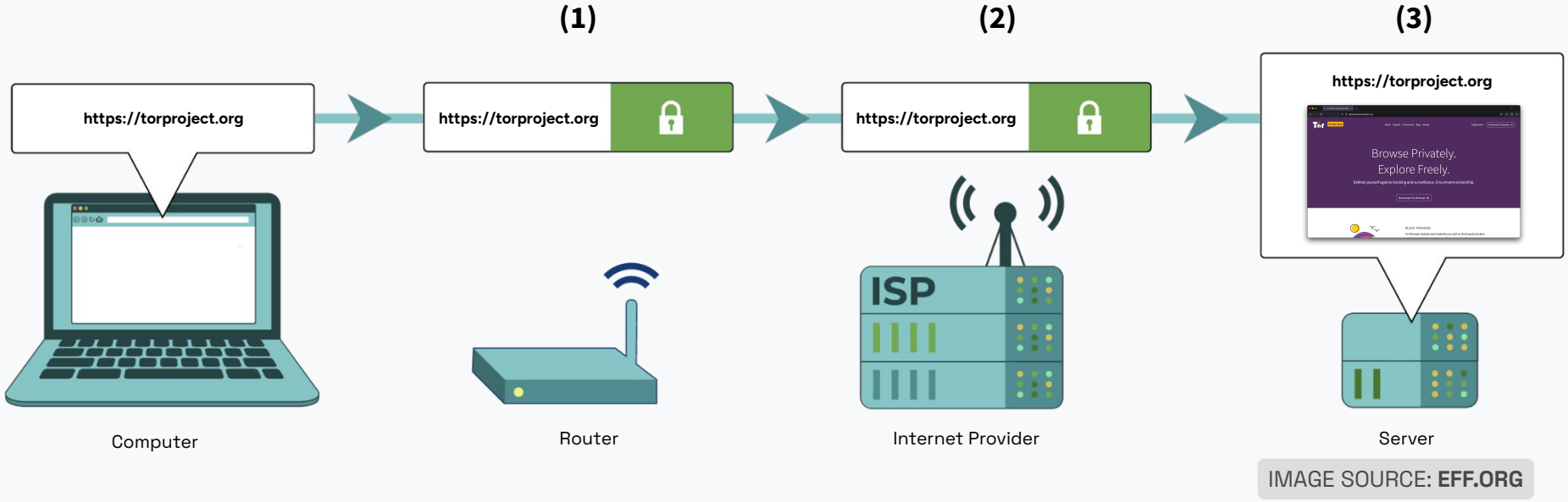


IMAGE SOURCE: **EFF.ORG**

Connecting to a Website Through a VPN

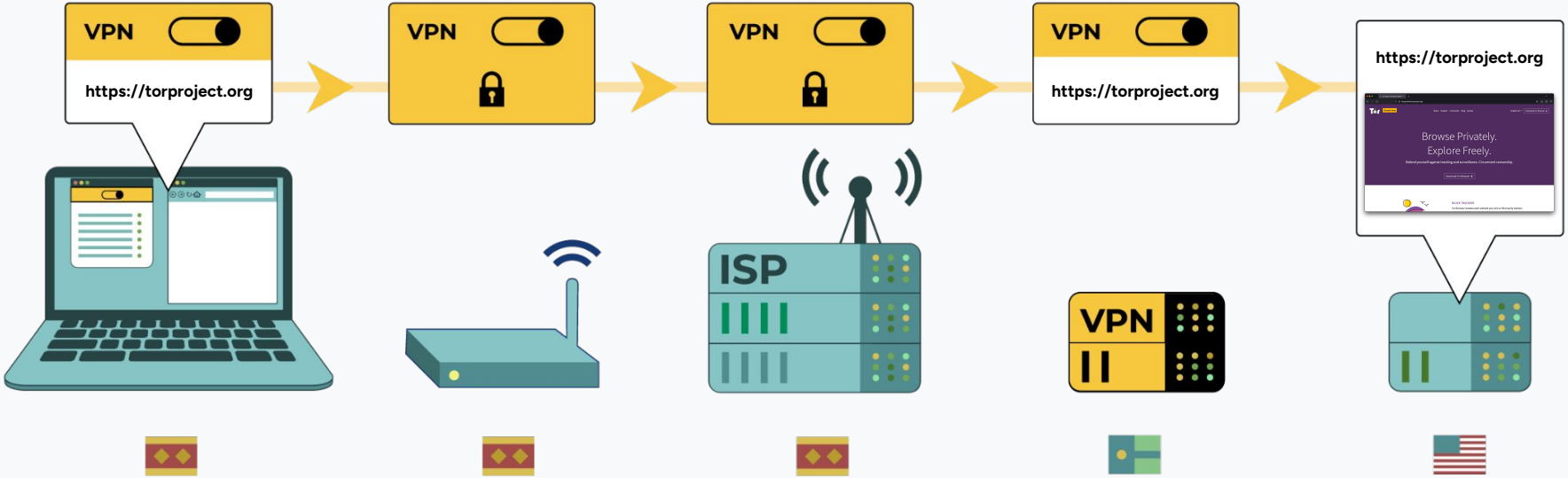


IMAGE SOURCE: **EFF.ORG**

Connecting to a Website Through Tor

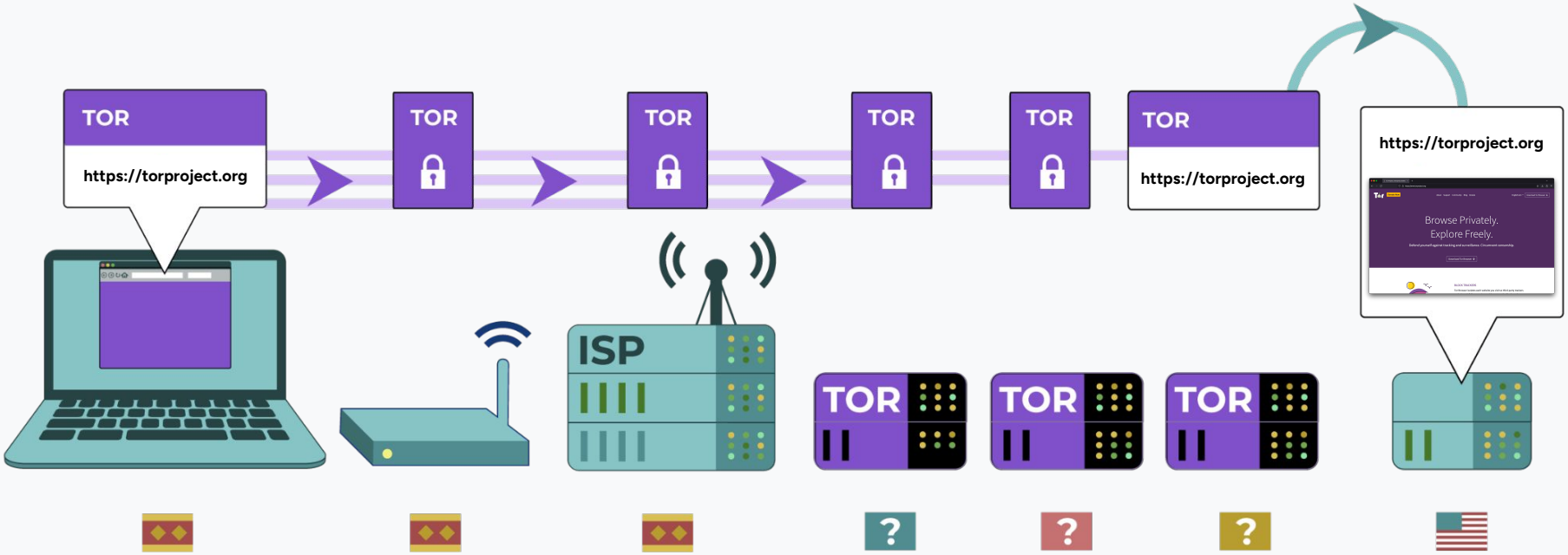


IMAGE SOURCE: **EFF.ORG**

VPN vs. Tor

- When using Tor, your traffic is routed through **3 servers instead of 1** such as through a VPN.
- Your traffic is **encrypted 3 times** and each server on the Tor network decrypts a layer.
- Tor servers are run entirely by volunteers instead of private corporations which tend to profit off of user data. Tor is therefore **decentralized** (VPNs aren't).

Privacy By Design

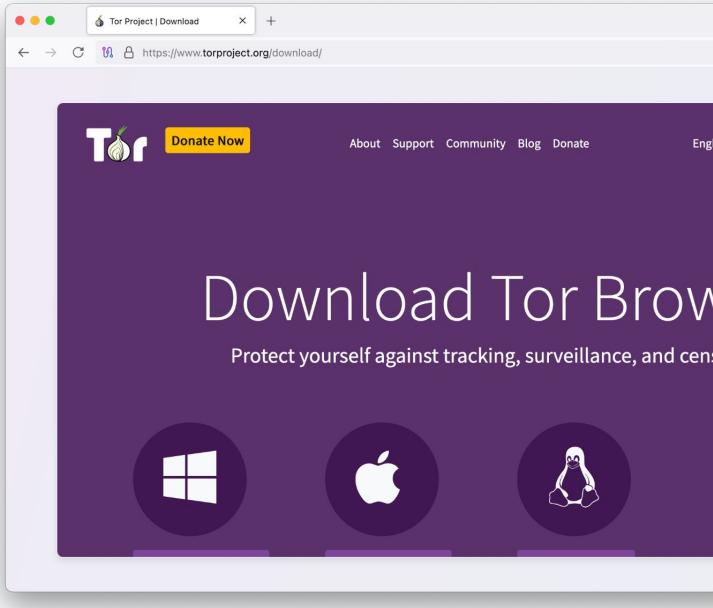
- Tor is completely **open source and free***, enabling privacy and security on the network through transparency of operation. Not all VPNs are open source or undergo independent security auditing.
- This makes a Tor connection **private by design**. Tor does not know who you are, where you are connecting from, and where you're going. No private data is stored.

** Free as in gratis, not freemium.*

3.
Using Tor Applications to Bypass Censorship

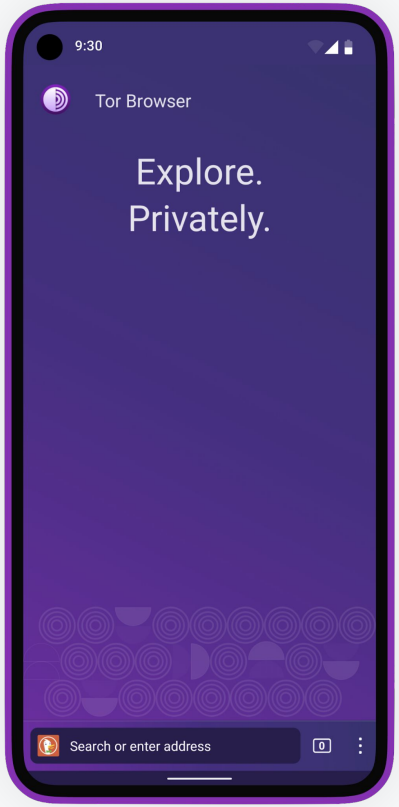
Tor Browser for Desktop

- Tor Browser is just like any other browser (Chrome, Firefox, Safari) except it **does not expose who you are and what websites you're visiting** to anyone surveilling your traffic.
- Tor Browser is available in 37 languages in a single **multi-locale** download.
- The safest way to download is from: https://torproject.org. Downloading Tor Browser from a **non-official source** is **dangerous**!



Tor Browser for Android

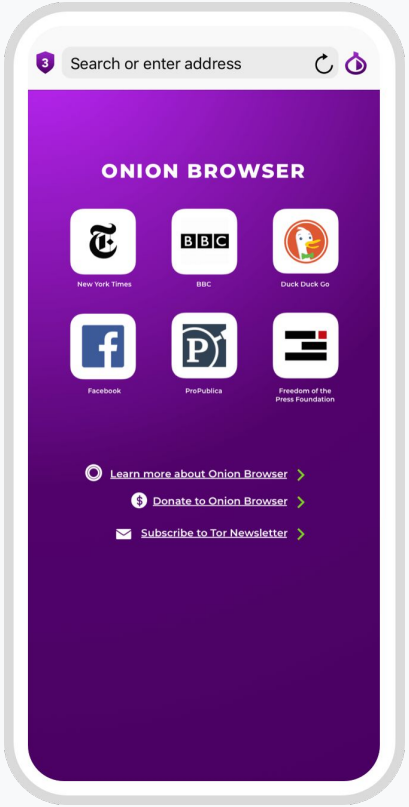
- Tor Browser for Android **resembles** Tor Browser for desktop in terms of features and protections. It is developed and maintained by the Tor Project.
- Users can download the application from the **Google Play** or **F-Droid** repository.
- Alternatively, users can download the .apk file from: https://torproject.org/download/



Onion Browser for iOS

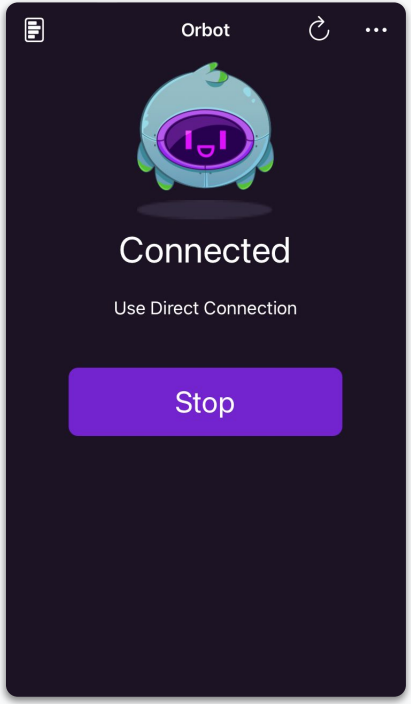
- Onion Browser is the **unofficial Tor browser** for iOS and the only one endorsed by the Tor Project.
- It is also **free and open source**, and is developed and maintained by The Guardian Project.
- There is no official browser called 'Tor Browser' for iOS → Be careful as **many fake Tor browsers** exist on iOS!
- Onion Browser is available through the Apple App Store: https://onionbrowser.com/

* Note: you need to download Orbot alongside Onion Browser for it to work as intended (see next slide).



Orbot for Android and iOS

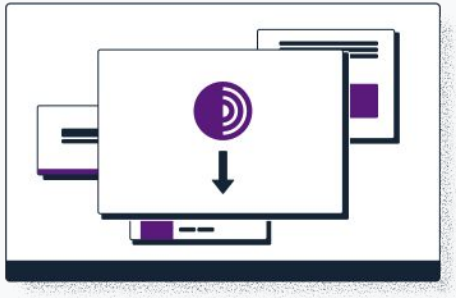
- Orbot is a mobile application that essentially routes **all your smartphone's traffic** through Tor, instead of just a browser going through Tor such as with Tor Browser.
- For example, you can **route apps** like Signal through Tor for enhanced privacy and security.
- It is developed and maintained by The Guardian Project as free and open-source software, and is available on both iOS and Android: https://orbot.app/



4.
When Tor is Blocked

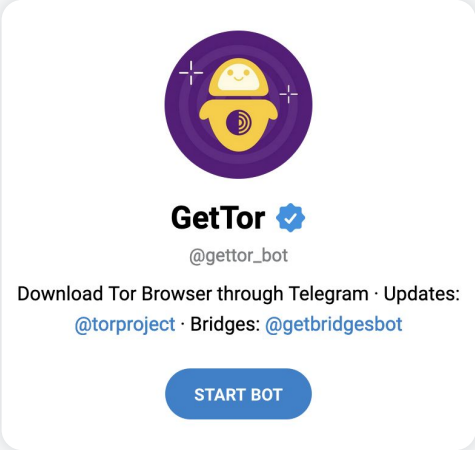
When torproject.org Is Blocked

- If https://torproject.org is **blocked**, try one of the official **mirror sites**:
  - https://tor.eff.org/
  - http://tor.calyxinstitute.org/ (if HTTPS is blocked)



When Mirrors Are Blocked

- Tor Project website and mirrors could be **blocked** on your network making it more difficult to download Tor Browser safely.
- The Tor Project has thus set up **alternative ways to download** Tor Browser. You can download it by:
  - Emailing GetTor to receive links to download Tor browser: gettor@torproject.org (works only from Gmail or RiseUp).
  - Messaging @GetTor on Telegram: https://t.me/gettor_bot



When Tor Itself Is Blocked

- Tor provides anti-censorship features called **bridges** for users to enable **when Tor is blocked** in a user's country or region.
- A **bridge** provides an alternative way to connect to the Tor network.
- It's basically a Tor entry relay, but its IP address is **not listed** on the public directory
- This makes it harder for Internet Providers (ISPs) and governments to block access to the bridge.
- Most bridges add an additional layer of masking called **Pluggable Transports** that disguise a bridges' Tor traffic by making it look like a regular connection rather than a Tor connection.

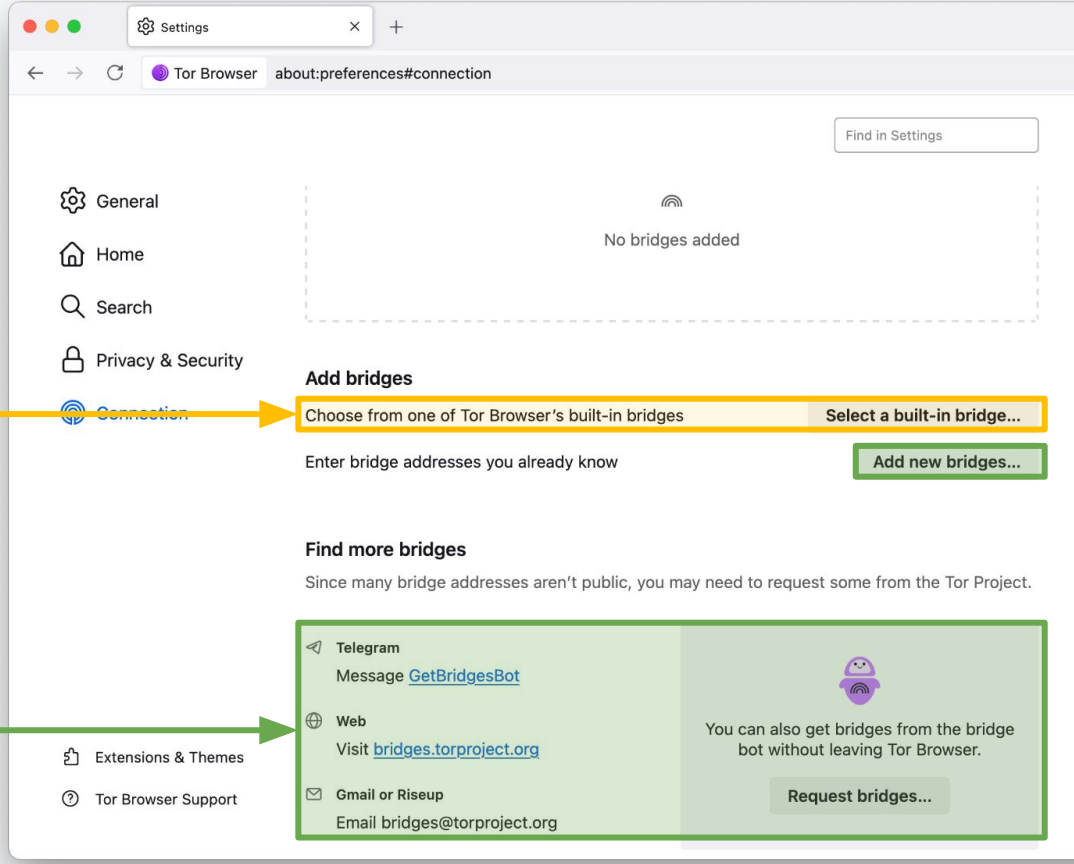
Bridges

Tor Browser includes powerful circumvention features called 'Bridges' for **getting around censorship of Tor**.

Here, users can choose from one of the default built-in bridges within Tor Browser.

Users can also request bridges through Tor's Telegram bot (@getbridgesbot), via email (bridges@torproject.org from Gmail or Riseup), or through Tor's website.

Once received, they can manually add the address in the 'Add new bridges' section above.



Pluggable Transports

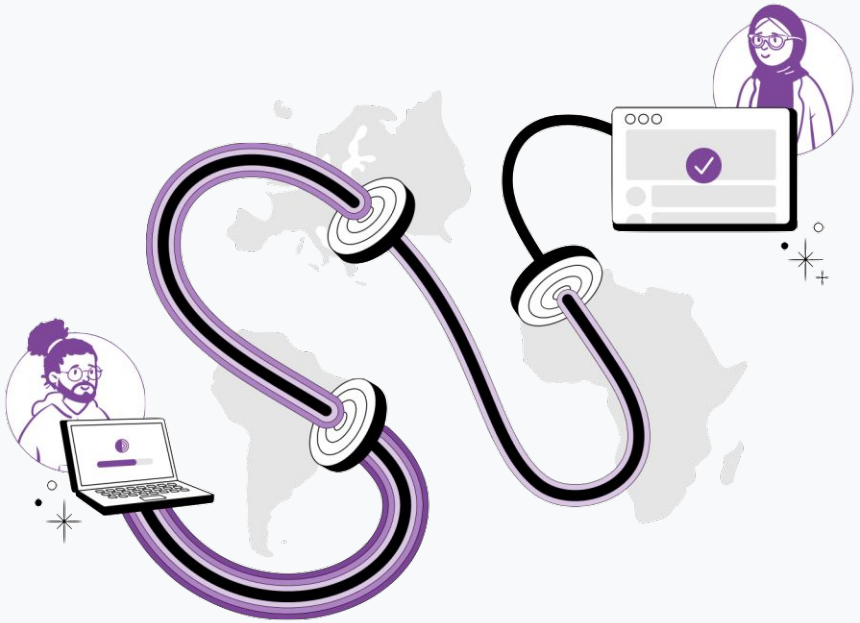
Anyone surveilling your internet traffic might be able to recognize patterns that indicate that you're connecting to Tor, and block your access to it (don't worry, they won't know what you intended to visit over Tor). Pluggable Transports prevent this by transforming Tor's traffic to look like something else entirely. The main types of pluggable transports on Tor are:

1. **obfs4:** makes Tor traffic look like random encrypted traffic (like nothing specific).
2. **meek-azure:** makes it look like you're connecting to a Microsoft service.
3. **snowflake:** makes your traffic appear that you're connecting to a videoconference (channels your traffic through volunteer-run proxies using WebRTC). For more on Snowflake: https://snowflake.torproject.org.
4. **WebTunnel:** mimics encrypted web traffic (HTTPS).

Enabling Bridges in Tor Apps

- On **Tor Browser for Desktop**, go to Settings > Connection > Bridges > select a bridge*
- On **Tor Browser for Android**, go to the gear icon (top right) > Config Bridge > select a bridge*
- On **Orbot for Android**, go to Use Bridges > select a bridge*
- On **Orbot for iOS,** go to the gear icon (top right) > Bridge Configuration > select a bridge*
- On **Onion Browser**, go to the gear icon (top right) > Bridge Configuration > select a bridge*

Thank you!



The Tor Project
Support Channels

Signal: https://signal.me/#p/+17787431312

Email: frontdesk@torproject.org

WhatsApp: https://wa.me/447421000612

Telegram: https://t.me/torprojectsupportbot

Forum: https://forum.torproject.org