

Testing & Evaluation Sheet	
Tor Browser	
<b>1. Tool Overview</b>	
Name:	Tor Browser
Category:	Browser
Purpose:	Tor Browser is a free, privacy-focused web browser that uses the Tor network to encrypt traffic and protect users' anonymity online.
Date	4/2/25
Status:	Deployed <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Operational - Actively running/maintained</li> <li><input type="checkbox"/> In Testing - Currently being evaluated or piloted</li> <li><input type="checkbox"/> Inactive/Deprecated - No longer maintained or functional</li> </ul>
Deployment Architecture:	<ul style="list-style-type: none"> <li><input type="checkbox"/> A standalone software - Runs entirely locally (e.g., runs on computer and doesn't depend on external server)</li> <li><input type="checkbox"/> A locally hosted service with separate server and client component - Run both backend/frontend yourself (e.g., backend could be on a local network, or self-hosted on cloud)</li> <li><input checked="" type="checkbox"/> A service with a local client that's hosted by a third party - You install a client on your device, but it connects to and depends on a remote server (e.g., Signal: install app (client), but Signal's servers handle message relaying, etc.)</li> </ul> <p><b>Tor Browser is a software that runs locally on a computer but connects to the Tor network to surf the web.</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> A service that is hosted by a third party but can also be self-hosted</li> </ul>
Version:	14.5a6
<b>2. Installation &amp; Setup</b>	
OS Compatibility	Windows, Linux, macOS, Android
Installation Manual:	Yes <a href="https://tb-manual.torproject.org/about/">https://tb-manual.torproject.org/about/</a>

Installation Steps:	<ol style="list-style-type: none"> <li>1. Open a search engine and enter "<b>Tor Browser</b>" or "<b>Download Tor Browser</b>" in the search bar.</li> <li>2. Click on the official "<b>Download Tor Browser</b>" link from the <b>Tor Project website</b>.</li> <li>3. On the download page, select the appropriate version for your operating system (Windows, macOS, Linux, or Android).</li> <li>4. Click the <b>Download</b> button and wait for the file to finish downloading.</li> <li>5. Once the download is complete, launch the installer, select your preferred language, and choose a destination folder for the installation.</li> <li>6. Follow the on-screen instructions to complete the installation process.</li> </ol> <a href="https://gitlab.torproject.org/tpo/applications/tor-browser">https://gitlab.torproject.org/tpo/applications/tor-browser</a>
Mention if command-line setup or special configurations are needed	There is no command line setup required for the Tor Browser as it comes with a graphical installer (command-line options are useful for scripting, automation, or advanced configurations but not necessary).
Common Installation Issues & Fixes:	<ol style="list-style-type: none"> <li>1. Troubleshooting Guide (provided by Tor):  <a href="https://tb-manual.torproject.org/troubleshooting/">https://tb-manual.torproject.org/troubleshooting/</a> </li> </ol>
User Documentation:	Yes
Required Technical Knowledge	Intermediate (an average user can easily install the browser and begin using it, but requires more technical knowledge on what configurations or security features to use).

### 3. Testing & Evaluation

<u>Category</u>	<u>Details</u>	<u>Score</u>
<b>Operational Functionality:</b>	<p><b>Functionality</b></p> <ul style="list-style-type: none"> <li>• The Tor Browser performs its intended function of properly avoiding surveillance and ensuring privacy while online. It routes internet traffic through a series of volunteer-run networks of relays in the Tor network. Each relay only knows its immediate predecessor and successor, making it extremely difficult to trace the full path back to the user — a technique known as onion routing.</li> <li>• Tor generally runs without broken features and bugs and large scale issues are uncommon as thousands of people contribute to running and maintaining the browser.</li> </ul>	

	<ul style="list-style-type: none"> <li>○ During testing, the Tor Browser was downloaded easily and web surfing was intuitive, showing no signs or bugs.</li> </ul> <p><b>Internet Dependence:</b></p> <ul style="list-style-type: none"> <li>● Does not have offline functionality (this is not a disadvantage as it is a tool for internet browsing).</li> <li>● Tor enables anonymous communication by hiding the user's IP address and directing it through a network of relays managed by volunteers.</li> <li>● 2G/3G networks: not recommended due to the slow speeds and high latency, which can make browsing and using Tor significantly slower and less reliable.</li> </ul> <p><b>Localization &amp; Language Support</b></p> <ul style="list-style-type: none"> <li>● Languages: Tor has published and translated this software for many different languages. There are 32 languages that have 90-100% of it translated <ul style="list-style-type: none"> <li>○ Chinese [Simplified &amp; Traditional], Thai, Vietnamese, Korean, Japanese</li> </ul> </li> </ul> <p><b>Mobile Accessibility</b></p> <ul style="list-style-type: none"> <li>● Optimized for mobile-accessibility, mainly for Androids</li> </ul>	
<b>Usability for Non-Technical Users</b>	<p><b>Ease of Installation &amp; Deployment</b></p> <ul style="list-style-type: none"> <li>● How easy is it to install &amp; configure? <ul style="list-style-type: none"> <li>○ The base installation is pretty easy for users following the steps above and the documentation provided. For those setting up Tor nodes or other privacy tools, the installation/setup is more complex.</li> </ul> </li> <li>● Are setup guides, manuals and FAQ's well maintained? <ul style="list-style-type: none"> <li>○ The setup guides, manuals, and FAQ's are well maintained and pretty extensive and a link to the manual is provided above.</li> </ul> </li> <li>● Time the installation process <ul style="list-style-type: none"> <li>○ 30 seconds</li> </ul> </li> </ul> <p><b>User Onboarding Experience</b></p> <ul style="list-style-type: none"> <li>● Does it provide documentation for first time users? <ul style="list-style-type: none"> <li>○ Tor maintains a sizable documentation repository that includes community guidelines and technical instructions especially for first time users.</li> </ul> </li> </ul>	

	<p><a href="https://tb-manual.torproject.org/running-tor-browser/">https://tb-manual.torproject.org/running-tor-browser/</a></p> <p><b>Technical Experience Level Required</b></p> <ul style="list-style-type: none"> <li>• Can non-technical users easily navigate the tool? <ul style="list-style-type: none"> <li>○ Tor is designed to be accessible to all users regardless of technical knowledge; however, non-technical users may find it more challenging to navigate and utilize the full anonymity and security capabilities. <ul style="list-style-type: none"> <li>■ Default: Tor attempts to connect without bridges.</li> <li>■ In heavily censored countries like China, direct connections are often blocked — not just technically, but politically risky. Even if the content of your traffic is encrypted and hidden, the mere fact that you're accessing the Tor network can be suspicious. Authorities may not know what you're doing, but they know you're doing something worth hiding — and that alone can draw unwanted attention.</li> <li>■ This might make non-technical users think Tor is unsafe without having the knowledge on bridges and pluggable transports like obfs4. Also, configuring some of these bridges or transports is unintuitive and not very heavily documented.</li> </ul> </li> </ul> </li> <li>• Is the interface intuitive? <ul style="list-style-type: none"> <li>○ The interface of Tor is very straightforward using the Tor Browser for advanced users. For non-technical users the privacy settings and security features may be a little confusing at first but the search engine is pretty intuitive.</li> </ul> </li> </ul>	
<b>Security &amp; Privacy Strength</b>	<p><b>Encryption Standards</b></p> <ul style="list-style-type: none"> <li>• What security protocols are used? <ul style="list-style-type: none"> <li>○ Multilayer Encryption (Onion Routing): Each packet encrypted three times before randomly being sent to three Tor nodes. In order to</li> </ul> </li> </ul>	

	<p>prevent any one node from knowing both the sender and the destination, each relay removes one layer of encryption, similar to peeling an onion.</p> <ul style="list-style-type: none"><li>○ Security Protocols: TLS 1.2+ → Protects client-entry node communication, AES-256 → Encrypted relay traffic, RSA-4096 → Secure key exchange &amp; relay authentication, SHA-3 → Data integrity verification, Diffie-Hellman → Perfect Forward Secrecy (unique session keys).</li></ul> <p><b>Censorship resilience</b></p> <ul style="list-style-type: none"><li>● Censorship Resistance: Tor has built in bridges that help users bypass censorship and access the Tor network in regions that it is blocked (More information in “Why is this useful to civil societies in authoritarian environments?” section).</li></ul> <p><b>Vulnerability: Its Resilience against known threats</b></p> <ul style="list-style-type: none"><li>● There are some potential vulnerabilities. They got a security assessment by Cure53 (cybersecurity company) and was published in January 2024 (they also provided suggestions).<ul style="list-style-type: none"><li>○ <a href="https://www.torproject.org/about/reports/">https://www.torproject.org/about/reports/</a><ul style="list-style-type: none"><li>■ Key risks included potential denial-of-service (DoS) attacks, user impersonation in chat services, and vulnerabilities in the Android app that could be exploited by malicious software on unpatched phones. These issues don’t undermine the core anonymity network itself but highlight the importance of keeping Tor tools updated and using them on secure devices.</li><li>■ <b>Bottom line:</b> For everyday users, Tor remains one of the best tools for anonymity — but, like any tech, it's not invincible. Staying updated and cautious is key.</li></ul></li></ul></li></ul> <p><b>Comparison with Known Standards</b></p> <ul style="list-style-type: none"><li>● One of the best softwares for anonymity is the Tor Browser. Tor is frequently suggested as a crucial tool for preserving privacy and resisting surveillance by</li></ul>	
--	---	--

	<p>the Electronic Frontier Foundation (EFF), a leading digital rights organization.</p> <p><b>Data Minimization</b></p> <ul style="list-style-type: none"> <li>As stated by their most recent audit, they only collect the necessary data and that data is being stored securely.</li> </ul> <p><b>Privacy Policy Accessibility and Clarity</b></p> <ul style="list-style-type: none"> <li>“Tor Browser prevents people from knowing the websites you visit. Some entities, such as your Internet Service Provider (ISP), may be able to see that you're using Tor, but they won't know where you're going when you do” (Tor Browser Privacy Policy)</li> </ul>	
<b>Maintenance/Sustainability</b>	<p><b>Community support</b></p> <ul style="list-style-type: none"> <li>There is a big and active forum with posts regarding feedback, support, news, etc. making it easy to get help and ask questions.</li> <li>However, the quantity and geographical distribution of relays run by volunteers have a significant impact on Tor's effectiveness. This underscores the need of local relay involvement for performance. <ul style="list-style-type: none"> <li>In Taiwan, there are lower numbers of volunteers running relays which may make Tor Browser slower.</li> </ul> </li> </ul> <p><b>Development active status</b></p> <ul style="list-style-type: none"> <li>Frequent updates ~ every month there is an update</li> <li>Status page that shows the current status of various sites of the TorProject, includes an incident history <ul style="list-style-type: none"> <li>■ <a href="https://status.torproject.org/">https://status.torproject.org/</a></li> </ul> </li> </ul> <p><b>Funding and Sponsorship</b></p> <ul style="list-style-type: none"> <li>Around \$7 million in disclosed funding</li> <li>Around 28.5% of the revenue was derived from individual donors, reflecting a growing base of grassroots support.</li> <li>Sponsorships: <ul style="list-style-type: none"> <li>Open Technology Fund</li> <li>Sida (Swedish International Development Cooperation Agency)</li> <li>Craig Newmark Philanthropies</li> <li>Ford Foundation</li> <li>Fastly (provides in-kind support for hosting Tor update)</li> </ul> </li> </ul>	

<p><b>Performance / Effectiveness &amp; Reliability</b></p>	<p><b>Testing Environment Setup:</b></p> <ul style="list-style-type: none"> <li>● <b>Device:</b> Dell XPS 15</li> <li>● <b>OS:</b> Windows</li> <li>● <b>Network:</b> 4G</li> </ul> <p><b>User Experience Observations</b></p> <ul style="list-style-type: none"> <li>● The tool felt relatively smooth when searching through the browser.</li> <li>● Tor Browser is sometimes slow but that is because of the extra layer of security and privacy using relay networks.</li> </ul> <p><b>Speed &amp; Responsiveness:</b></p> <ul style="list-style-type: none"> <li>● Tor's usage of numerous relays to transport traffic can make it sluggish. Speed is frequently slower than with conventional surfing techniques, particularly when visiting highly blocked areas or during periods of high traffic. <ul style="list-style-type: none"> <li>○ For example, it could be substantially slower to download reports, access secure communication networks, or even open human rights websites with a lot of documents. Compared to standard internet rates of 25–100 Mbps, Tor's download speeds were between 0.5 and 2 Mbps, which is three to five times slower than ordinary surfing. This might provide difficulties when working in settings where every minute matters, such as those with strict internet control and surveillance, or while doing time-sensitive tasks.</li> </ul> </li> </ul> <p><a href="https://surfshark.com/blog/tor-browser-slow">https://surfshark.com/blog/tor-browser-slow</a></p> <p><b>Resource Usage:</b></p> <ul style="list-style-type: none"> <li>● Tor uses a moderate amount of resources. Because of the relays, it consumes more resources than a standard browser, although it's not overly demanding. When functioning as a relay node, it may use a lot of resources.</li> </ul> <p><b>Network Performance:</b></p> <ul style="list-style-type: none"> <li>● Tested network efficiency by monitoring bandwidth consumption with tools like Wireshark.</li> <li>● Tor increases latency and reduces bandwidth due to the onion-routing mechanism that bounces traffic through multiple relays. <ul style="list-style-type: none"> <li>○ 100 ms - 30 seconds (Latency depending on usage)</li> </ul> </li> </ul> <p><a href="https://metrics.torproject.org/torperf.ht">https://metrics.torproject.org/torperf.ht</a></p>	
---	---	--

	<p><a href="https://www.onion.city/ml?start=2025-01-01&amp;end=2025-04-01&amp;server=onion&amp;filesize=50kb">ml?start=2025-01-01&amp;end=2025-04-01&amp;server=onion&amp;filesize=50kb</a></p> <ul style="list-style-type: none"> <li>■ 1-10 Mbps (Bandwidth)</li> </ul> <p><b>Reliability</b></p> <ul style="list-style-type: none"> <li>● Since the community is large and in general it is well liked.</li> <li>● 3rd party cybersecurity audits demonstrate the security functions of Tor and provide feedback on the weaknesses and ways to improve.</li> </ul>	
<p><b>Deployment Considerations:</b></p>	<p><b>Open Source &amp; Transparency:</b></p> <ul style="list-style-type: none"> <li>● The code is available for independent verification.</li> </ul> <p><b>Cloud vs. Local Deployment:</b></p> <ul style="list-style-type: none"> <li>● Designed for local use and doesn't need AWS/Azure.</li> <li>● Can be run on a cloud server but like a Tor relay or exit node, not as a typical web browser.</li> <li>● Tor is currently deployed so users do not have to redeploy if they want to use it and is actively maintained (security updates every few weeks and major updates annually), aligned with Firefox ESR (Extended Support Release) updates.</li> </ul> <p><b>Dependencies:</b></p> <ul style="list-style-type: none"> <li>● No, the Tor Browser itself does not require Docker, Python, or databases.</li> <li>● However, the Tor network and related services may have dependencies: <ul style="list-style-type: none"> <li>○ The Tor daemon (tor), which powers the network, is written in C and does not require Docker or a database.</li> <li>○ Some Tor tools and scripts (e.g., Onion Services management) may use Python or other scripting languages.</li> <li>○ Running a Tor relay or exit node on a server does not need a database but may require specific system configurations.</li> </ul> </li> </ul> <p><b>Post-Deployment Maintenance</b></p> <ul style="list-style-type: none"> <li>● Yes, it is easy to maintain after deployment.</li> <li>● If code is forked, modifying the browser's interface is similar to Firefox ESR and not too difficult. If attempting patches for security/networking changes, that would require much more expertise.</li> </ul> <p><b>Merge/Sustainability:</b></p>	

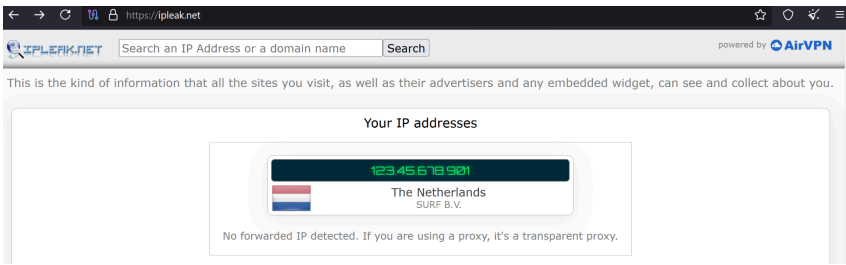


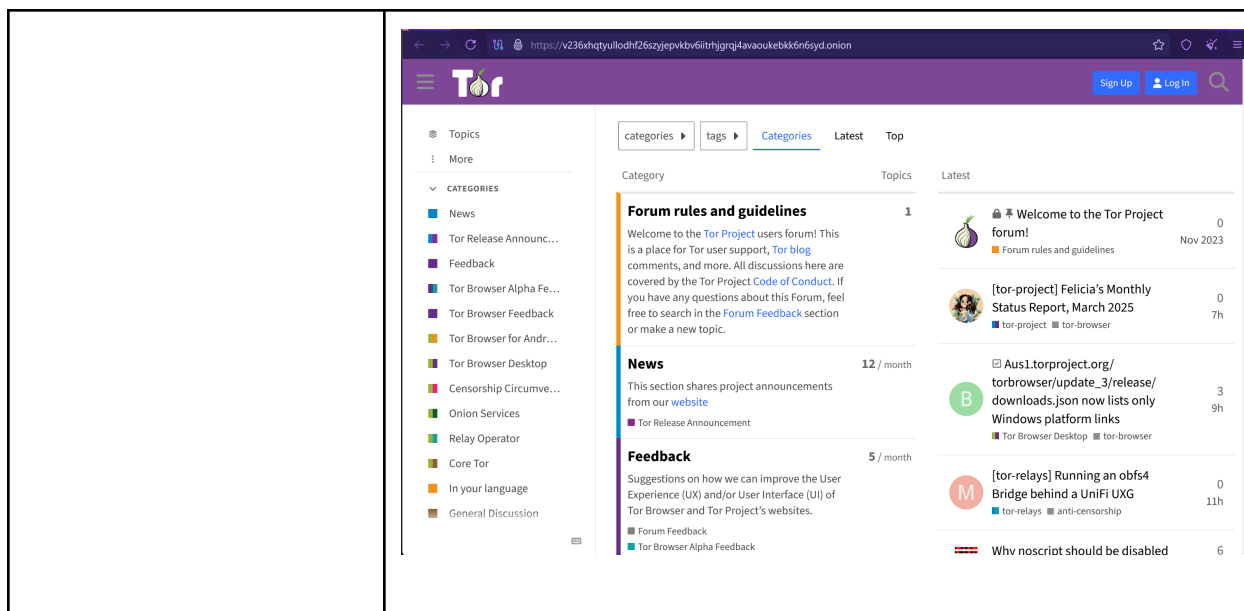
	<ul style="list-style-type: none"> <li>• How open is the original project to contributions? <ul style="list-style-type: none"> <li>○ The Tor Project is open-source and welcomes contributions. The source code is available on GitLab: <a href="https://gitlab.torproject.org/">https://gitlab.torproject.org/</a>.</li> <li>○ Developers can contribute by submitting patches, bug fixes, or new features.</li> <li>○ The project has public issue tracking, a developer guide, and active maintainers reviewing changes.</li> </ul> </li> <li>• Is it easy to submit changes back to the main repository? <ul style="list-style-type: none"> <li>○ Moderate difficulty—while contributions are welcome, Tor has strict security and privacy requirements.</li> <li>○ Code changes undergo extensive review before merging.</li> <li>○ Some contributions (especially security-related) require deep knowledge of network security and anonymity systems.</li> <li>○ Contributors should follow the <a href="#">Tor Project's coding guidelines</a>.</li> </ul> </li> </ul>	
--	---	--

#### 4. Testing Scenarios

<ul style="list-style-type: none"> <li>• <b>Scenario 1</b> IP Leak Testing <a href="https://ipleak.net/">https://ipleak.net/</a></li> </ul>	 <p>The screenshot shows the Ipleak.net website interface. At the top, there's a search bar and a 'powered by AirVPN' logo. Below, a message states: 'This is the kind of information that all the sites you visit, as well as their advertisers and any embedded widget, can see and collect about you.' The main section, 'Your IP addresses', displays a masked IP address '123.456.789.010' and identifies the location as 'Taiwan - Taipei City' with the 'Taiwan Academic Network, Taiwan Information Center'. It notes 'No forwarded IP detected. If you are using a proxy, it's a transparent proxy.' Below this, it shows 'Browser default: IPv4 (250 ms)' and 'Fallback: Fail (timeout)'. The 'Your IP addresses - WebRTC detection' section at the bottom indicates that if connected to a VPN and seeing the ISP IP, the system is 'leaking WebRTC requests'.</p>
---	---

*Figure 1: Public IP address using Google Chrome (Actual IP masked due to security reasons)*

	<div data-bbox="581 205 1421 468">The screenshot shows the IPLeak.net website. At the top, there's a search bar with the text "Search an IP Address or a domain name" and a "Search" button. Below the search bar, a message states: "This is the kind of information that all the sites you visit, as well as their advertisers and any embedded widget, can see and collect about you." The main content area is titled "Your IP addresses" and displays a box with the IP address "123.456.78.901" in green text. Below the IP address, it shows a flag for The Netherlands and the text "The Netherlands SURF B.V.". At the bottom of the box, it says "No forwarded IP detected. If you are using a proxy, it's a transparent proxy."</div> <p><i>Figure 2: Public IP address using Tor (Actual IP masked due to security reasons)</i></p> <ul style="list-style-type: none"><li>● <b>Windows:</b> Open Command Prompt (Win + R, type cmd, hit Enter), then type <b>ipconfig</b> and look for IPv4 Address under your active network connection.</li><li>● <b>Mac:</b> Open Terminal and type <b>ipconfig getifaddr en0</b> (use en1 for Ethernet), then note your private IP.</li><li>● <b>Linux:</b> Open Terminal and type <b>ip a</b>, then look for <b>inet</b> under your active network interface.</li><li>● As shown in Figure 1 above, Chrome does not block or mask my actual IP address, making it traceable and revealing detailed geolocation information. In addition to compromising privacy, this exposure can locate me within a short radius. This puts the safety and private information of journalists, campaigners, and human rights defenders who want to remain anonymous at serious risk.</li><li>● As shown in Figure 2 above, Tor effectively masks my actual IP address, preventing it from being traced back to me. Tor makes it almost impossible to determine my exact location by passing my connection via several encrypted bridges rather than disclosing my actual location. This improves security and most importantly privacy, offering crucial protection for journalists, activists, and human rights advocates who must maintain their anonymity.</li></ul>
<ul style="list-style-type: none"><li>● <b>Scenario 2</b> Example of Onion service</li></ul>	<p>Onion service directories like Ahmia and the Hidden Wiki list various onion services. You can also use search engines that index onion service.</p>



## 5. Insights & Recommendations

### Key Findings

### Strengths:

- Easy to download and use
- Can hide IP address
- Individuals can submit merge requests (pull requests equivalent in GitLab) and this follows Tor's contributions guidelines and strict security standards.
- Not all changes are accepted and security and anonymity are top priorities.
- Small fixes (like UI changes) can be merged with review.
- Modifications like networking and cryptography require much more extensive review and testing before they are accepted.
- Settings → Connections → Bridges:
  - Tor has built in bridges that help users bypass censorship and access the Tor network in regions that it is blocked.
  - Normally Tor clients connect to publicly known entry nodes but bridges act as hidden entry points which are not publicly listed making it harder to censor and block them.
  - Tor Browser includes some specific types of bridges known as “pluggable transports”, which can help conceal the fact you're using Tor.
  - obfs4:
    - Makes your Tor traffic look like random data. May not work in heavily censored regions.

	<ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li>■ Disguises Tor traffic to prevent deep packet inspection (DPI) from detecting it.</li> </ul> </li> <li>○ Snowflake:           <ul style="list-style-type: none"> <li>■ Routes your connection through Snowflake proxies to make it look like you're placing a video call, for example.</li> <li>■ Volunteer-based evasion, using volunteers' browsers as proxies</li> <li>■ Hard to block as proxies constantly change</li> </ul> </li> <li>○ meek-azure:           <ul style="list-style-type: none"> <li>■ Makes it look like you're connected to a Microsoft website, instead of using Tor. May work in heavily censored regions, but is usually very slow.</li> <li>■ Cloud based evasion, routing traffic through cloud services</li> <li>■ Slower than obfs4 but works in much higher restrictive environments.</li> </ul> </li> <li>○ Benefits of Bridges:           <ul style="list-style-type: none"> <li>■ Bypass censorship where Tor is blocked</li> <li>■ Prevents ISP (Internet Service Provider) tracking</li> <li>■ Onion services (often called the dark web) are websites that use .onion domains and are only accessible through the Tor network. If public guard nodes are blocked, onion services cannot be accessed. Bridges act as secret entry points, allowing users to bypass these blocks and connect to onion services anonymously.</li> <li>■ If a country blocks Tor access, a journalist or activist can use a bridge to connect and securely visit onion sites (e.g., privacy tools, whistleblower platforms, or independent news sources).</li> <li>■ Help others access free and open internet by hosting a bridge. This is a volunteer-based node that helps censored users in restricted countries connect to Tor. This supports online freedom, enhancing privacy for activists, journalists, and researchers in oppressive regimes.</li> </ul> </li> <li>○ Onion Services:</li> </ul>
--	---

	<ul style="list-style-type: none"> <li>■ Allows websites and services to be hosted anonymously without revealing location or IP address (Ex. example.com-&gt;asdf123.onion and only accessible through Tor browser)</li> <li>■ When visiting such a website, your request is routed through multiple relays, keeping both the website owner and person accessing it anonymous.</li> <li>■ Enables individuals to carry out their job without worrying about being tracked, including NGOs, civil society groups, and whistleblowers.</li> <li>■ This promotes censorship resistance in nations that restrict websites and privacy as no central authority is aware of who owns or views the website.</li> </ul> <p><b>Weaknesses:</b></p> <ul style="list-style-type: none"> <li>● According to 2024 3rd party audit ‘documentation could be improved to clarify the commitment to user privacy and avoid any potential data leaks’ &amp; ‘A formal code review process ought to be implemented, focusing on privacy implications for all changes. This process should include peer reviews, automated privacy checks, and regular audits to ensure privacy considerations are consistently addressed during development.’</li> <li>● Websites can limit down their search results if they can determine that you have a different screen resolution than other users. For this reason, running Tor in full screen mode is not advised nor is installing any browser extensions.</li> <li>● Although Tor exclusively secures communication within the Tor Browser, many users mistakenly think it encrypts all of their data. Tor does not cover any other apps, like Zoom or Spotify.</li> <li>● Tor helps protect your privacy online, but it can't protect you if your device is already infected — like if someone installed a keylogger or screen recording malware on your computer.</li> <li>● Do not log into personal accounts (Gmail, Facebook, Instagram, etc.) or download documents while using Tor as it breaks anonymity.</li> </ul>
<b>Suggested Improvements</b>	<ul style="list-style-type: none"> <li>● User Interface Improvements: UI changes to improve clarity and navigation <ul style="list-style-type: none"> <li>i. Enhance dark mode support and accessibility options.</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>Documentation: Step-by-step installation guides, tutorials for technical users <ul style="list-style-type: none"> <li>More interactive tutorials for technical users (e.g., setting up a Tor relay or Onion Service).</li> </ul> </li> </ul>
<b>Alternative Tools:</b>	Brave, Mullvad, Librewolf
<b>License:</b>	Mozilla Public License
<b>Cost/Resource Implications</b>	<b>Total Cost of Ownership:</b> <ul style="list-style-type: none"> <li>All features of Tor are free</li> <li>No subscription required.</li> </ul>
<b>Why is this useful to civil societies in authoritarian environments?</b>	<ul style="list-style-type: none"> <li><b>Platform protection/Censorship:</b> <ul style="list-style-type: none"> <li>National firewalls in nations like China prevent access to websites that discuss democracy, human rights, and independent journalism. Because authorities in these areas ban known Tor nodes, Tor is frequently unreachable due to its typical setup. Tor bridges, which are unpublished relays not included in the public directory, are what users must rely on. Deep packet inspection (DPI) may, however, identify and block even these.</li> <li>To get around censorship and combat that, Tor provides pluggable transports like obfs4, which trick DPI systems by making Tor traffic appear to be random data. Even then, advanced censorship systems like China's Great Firewall are able to identify and block obfs4.</li> <li>To overcome that, users need to request private (unlisted) obfs4 bridges that are distributed through Tor's BridgeDB service or email. <ul style="list-style-type: none"> <li><a href="#">Tor's BridgeDB service</a> (site may be blocked so email option might be more reliable)</li> <li>Send an email to: <a href="mailto:bridges@torproject.org">bridges@torproject.org</a> <ul style="list-style-type: none"> <li>Subject line and body: Write "<b>get transport obfs4</b>"</li> <li>Important: You must send the email using a Gmail address. (Other email providers may be blocked or rejected.)</li> </ul> </li> <li>To configure, open Tor and click "<b>Configure Connection...</b>" rather than "<b>Connect</b>". Then, paste the bridge lines (Keep switching bridges regularly if they stop working or get blocked).</li> </ul> </li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>○ An NGO employee in Beijing, for instance, can manually configure Tor with a custom obfs4 bridge to avoid the Great Firewall's detection when attempting to access a restricted international human rights website. This enables safe cooperation with partners overseas, advocacy resources, and ongoing access to outside news.</li> <li>● <b>Identity protection through onion services:</b> <ul style="list-style-type: none"> <li>○ Activists and whistleblowers at risk of arrest or retaliation can use <b>onion services</b> to host or access content without revealing their location. For example, an NGO that documents military abuses in Myanmar, for example, can create a .onion site to safely collect civilian testimony, protecting both sides from IP monitoring and domain takedowns.</li> <li>○ Tor encrypts data and anonymizes its path, making it more difficult for authoritarian governments to track down communications or determine who is accessing what in monitored situations. For CSOs working in nations like Iran, where ISPs are obligated to monitor traffic and report suspected behavior, this is very helpful. Through onion services, Tor can allow these organizations to securely communicate encrypted emails, share documents, and use prohibited programs like Signal or ProtonMail.</li> </ul> </li> <li>● It is also recommended to use a working VPN (if not illegal in the country) before starting the Tor browser to make it more difficult for firewalls to detect and block Tor.</li> <li>● If obfs4 bridge does not work, try Snowflake (WebRTC-based Transport) or Meek (Cloud-based Transport) bridges as well. <ul style="list-style-type: none"> <li>○ WebRTC technology is more resistant to blocking than other transports.</li> <li>○ Cloud-based transport is hard to block because it disguises Tor traffic as common HTTPS traffic to well-known cloud providers, such as Google or Amazon Web Services and can be a very effective option in regions with advanced censorship techniques.</li> <li>○ If these still do not work, you may need to set up your Tor bridge if you have access to a server outside the country using Tor's official bridge setup guide.</li> </ul> </li> </ul>
--	--