Understanding Internet Censorship and Surveillance

The internet relies on many interconnected systems working together to deliver your communications from one place to another. When someone attempts to block parts of the internet or restrict certain activities, they can target multiple layers of this system. Their methods depend on the technology they control, their resources, and whether they have the authority to compel others to act.

Surveillance and Censorship: Two Sides of the Same Coin

Internet censorship is essentially a two-step process: spotting "unacceptable" activity, and then blocking it. Detecting activity is a form of surveillance. If network administrators can see where you're going online, they can decide whether to restrict access. Tools that protect privacy also make censorship more difficult. Many circumvention tools also protect your data from eavesdroppers.

The Cost of Surveillance

Blocking internet traffic has consequences. Over-blocking can be even more damaging. For example, the Chinese government does not block GitHub, even though it hosts anti-government content, because developers rely on it and blocking it would harm the economy. Other governments make different choices, including temporary internet shutdowns that can severely impact local economies.

Circumvention Techniques

The best circumvention method depends on your location and the type of censorship you face. Tools like OONI Probe can help identify blocking methods, but using them may draw attention.

Using encryption makes selective blocking harder. Technologies like HTTPS and encrypted DNS protect more of your browsing information.

Change Your DNS Provider and Use Encrypted DNS

- • Changing DNS providers can bypass DNS-based blocking, but your new provider will see your DNS activity.
- • Encrypted DNS prevents network actors from seeing or altering DNS traffic, though some governments block known encrypted DNS endpoints.
- • Browsers like Firefox, Chrome, Edge, and operating systems like Android, iOS, and macOS support encrypted DNS.

Use a VPN

A VPN encrypts your traffic and routes it through another server, sometimes in another country. This can bypass regional blocks, but VPN providers can still see your activity. Depending on your threat model, governments may access VPN logs. VPNs may not work against all types of censorship.

Using the Tor Browser

Tor routes your traffic through multiple relays, hiding your identity and helping bypass censorship. However, observers can see that you are using Tor. Tor may be slow or blocked in some regions. Tor’s Connection Assist can help users connect via bridges. Always download Tor from the official website.

Use Proxy Servers for Messaging Apps

If apps like WhatsApp or Signal are blocked, proxy servers can help you access them. Messages remain end-to-end encrypted, but proxy operators can see your IP address.