What is Internet censorship?

Internet censorship is the **intentional control** or suppression of what can be accessed, published, or viewed on the internet.

OONI measures censorship on the **network** level, involving the **blocking of websites and apps.**

Why measure Internet censorship?

1. Check/confirm reports
2. Uncover information controls
3. Transparency and oversight
4. Collect evidence of information controls

OONI

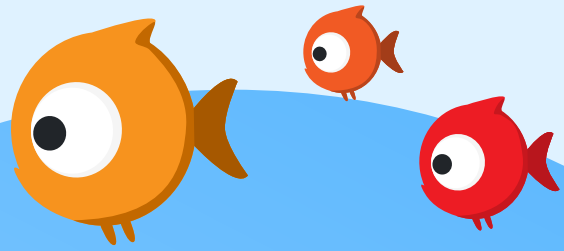
Founded in 2012, the Open Observatory of Network Interference (OONI) is a non-profit free software project documenting Internet censorship around the world.

Learn more about OONI: ooni.org

OONI

Understanding Internet Censorship

Exploring Web Restrictions and Access Control



Who implements Internet censorship?

Internet Service Providers (ISPs) can use a variety of censorship techniques. These include **DNS tampering**, **IP blocking**, **SNI filtering**, among others.

How is Internet censorship implemented?

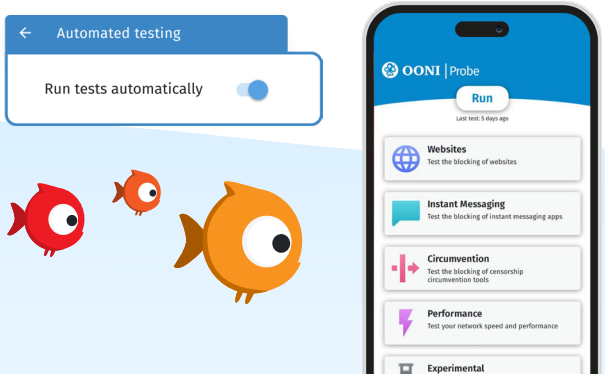
Internet Service Providers (ISPs) block access to specific websites and/or applications based on government orders and/or in compliance with national legislation.

How to measure Internet censorship?

Get the **OONI Probe** app on Mobile and Desktop.

Scan to Install OONI Probe →

Enable **Automated testing** in the settings to have tests run automatically every day!



DNS tampering

DNS tampering occurs when Internet Service Providers (ISPs) interfere with the DNS resolution for a particular hostname, preventing you from accessing it (e.g. by returning the wrong IP address).

IP blocking

IP blocking occurs when Internet Service Providers (ISPs) **block connections to the IP address** of a website.

HTTP blocking

HTTP blocking occurs when an ISP **interferes with the connection between your computer and the server hosting the website** you're trying to access.

This can be implemented by intercepting your HTTP request (in some cases, redirecting you to a block page) or by closing the connection (thereby preventing the normal exchange between your computer and the server of the website).

SNI-based filtering

SNI is an extension for the TLS protocol (used for websites hosted on HTTPS), designed to specify what hostname the encrypted connection should be established with.

As the SNI field is unencrypted, ISPs are able to see if you are trying to access a banned website and restrict access (for example, by closing the connection).

Censorship that is **informed by the SNI field** is characterised as SNI-based filtering.

	Blocking method					
Detection method	Closing the connection (RST or FIN)	Packet dropping	Traffic throttling	MITM	Bad HTTP response	Bad DNS answer
Destination IP (+ port)	✓	✓	✓	✓		
Domain in DNS query						✓
HTTP Host header	✓	✓	✓	✓	✓	
SNI field in TLS handshake	✓	✓	✓	✓		